FPKIPA
Federal Public Key Infrastructure Policy Authority

COMMON Certificate Policy Change Proposal Number: 2020-02

To: Federal PKI Policy Authority (FPKIPA)
From: Federal PKI Certificate Policy Working Group (CPWG)
Subject: Proposed modifications to the Federal PKI Common Policy Framework Certificate Policy and certificate profile specification
Date: August 19, 2020

Title: Consolidated update to Common Policy and associated profiles

Version and Date of Certificate Policy Requested to be changed:

- *X.509 Certificate Policy For The Federal PKI Common Policy Framework Version 1.32, April 14, 2020*

Change Advocate's Contact Information:
Organization: FPKI Policy Authority
E-mail address: fpki@gsa.gov

Organization requesting change: FPKI Certificate Policy Working Group

Change summary: This is a comprehensive update to Common Policy and the associated certificate profile specification (formerly titled "X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program"). High-level update summary:

- Removed Foreword
- Standardized terminology
- Realigned requirements with appropriate policy sections
- Increased use of tables to improve readability
- Aligned requirements with observed agency practices
- Clarified definitions of certificate types
- Streamlined certificate naming
- Updated certificate re-key, renewal, and modification definitions for clarity
- Removed SHA-1 references
- Updated permitted key sizes and algorithms
- Converted sections after Section 9 to appendices
- Updated format and content of certificate profiles
    - Aligned profiles with proposed updates to Common Policy
    - Added "Common PIV-I" profiles

  - Split Cross Certificate profile into two profiles (Cross certificate and Intermediate CA) to help clarify requirements and reduce confusion
  - Numerous worksheet updates (see Appendix C)

Background: This update consolidates CPWG policy recommendations dating back to 2018. It also cleans-up outdated references and requirements, clarifies existing requirements, aligns policy with observed agency practices (e.g., certificate naming), and improves readability.

Updates related to the following topics were discussed with CPWG members to minimize adverse impact:

- Authorization data in subscriber certificates
- Federal subscriber certificate naming
- Time to process certificate applications
- Updated CA rekey timelines
- Updated references for permissible options comparable to "digitally signed attestation under perjury" requirement (declaration of identity)
- Permitted key sizes and algorithms
- Identification and authentication requirements for routine subscriber re-key
- CA cryptographic module requirements
- Certificate profile changes

Additional detail related to update activities and milestones is included in Appendix A.

Specific Changes: Due to format changes and the number of edits, updates were highlighted to CPWG and FPKIPA members in separate, redlined versions of Common Policy.

Change Impact:

- Potential impacts resulting from the proposed updates to Common Policy are included in Appendix B.
- Potential impacts resulting from the proposed updates to the certificate profiles are included in Appendix C.

Estimated Cost: TBD

Implementation Date: September 1, 2021

Prerequisites for Adoption: None

Plan to Meet Prerequisites: Not applicable

Approval and Coordination Dates:
Date presented to CPWG: January 14, 2020
Date change released for comment: February 17, 2020
Date comment adjudication published: August 19, 2020

Appendix A: Update Activities and Milestones

Q3 FY 2019
(1Apr - 30Jun)

- May CPWG - Call for policy updates and clean-ups (5/28/19)
- FPKIPA Support Team began section by section review of Common Policy and Profiles

Q4 FY 2019
(1Jul - 30Sept)

- FPKIPA Support Team continued section by section review of Common Policy and Profiles
- September CPWG - Discussions related to *Authorization Data* and *Certificate Naming*
- FPKIPA Support Team began draft updates

Q1 FY 2020
(1Oct - 31Dec)

- FPKIPA Support Team continued draft updates
- November CPWG - Discussions related to *Time to Process Applications* and *Permitted Algorithms* (11/26/19)
- FPKIPA Support Team draft finalization and internal review

Q2 FY 2020
(1Jan - 31Mar)

- FPKIPA Support Team comment adjudication
- January CPWG - FPKIPA Support Team shares status update and requests additional feedback (1/28/20)
- FPKIPA Support Team shares policy artifacts for CPWG feedback (2/17/2020)
- March CPWG - Review period extended one month (4/28/20).

Q3 FY 2020
(1Apr - 30Jun)

- April CPWG - Review feedback and proposed adjudication (4/28/20)
- FPKIPA Support Team comment adjudication, incorporation of 2020-01, and distribution of Draft Release #2 (5/22/20)
- May CPWG - Summarized comment adjudication and reviewed next steps (5/28/20)
- June PA - Change proposal introduction to facilitate discussion on implementation timeline and cost (6/9/20)
- Draft Release #3 (6/18/20)
- June CPWG - Summarized recent updates and reviewed next steps (6/23/20)

Q4 FY 2020
(1Jul - 30Sept)

- Draft Release #4 (7/13/20)
- July PA - Finalized change proposal and initiated vote (7/14/20)
- August PA – Discussed agency feedback and next steps (8/11/20)
- Change proposal finalized and initiated vote (8/19/20)

APPENDIX B: IMPACT OF POLICY UPDATES

Policy Change Summary	Impact
Overall • Standardized terminology ("Human Subscriber", "Device", "must", "publicly accessible", etc.) • Clarified and streamlined language • Standardized formatting of "Practice Notes" and external references • Removed references to "legacy" agency PKIs, deprecated algorithms (e.g., SHA-1), and deprecated policies (e.g., M-04-04) • Relocated requirements to more applicable policy sections	No negative impact
Section 1 • Tabularized, re-ordered, and clarified policies covered by the CP • Updated scope of CP to remove code signing and only locally trusted CA use cases	No negative impact
Section 2 • Clarified Authority Information Access (AIA) and Subject Information Access (SIA) requirements • Added option for single DER encoded certificate file (AIA)	No negative impact
Section 3 • Reorganized certificate subject name and subject alternative name requirements into independent sub-sections • Updated naming requirements to align with observed agency practices • Removed unused name types (e.g., DC=mil) • Incorporated changes proposed in draft "Updated registration processes and biometric linkage" Change Proposal (June 12, 2019) • Included reference to FIPS 201 for the purposes of human subscriber identity proofing • Removed references to authorizations in subscriber certificates	No negative impact
Section 4 • Timeframe for certificate application process modified from 30 days to 90 days; topic discussed with CPWG • Clarified definitions of "renewal", "re-key", and "modification" • Tabularized CRL issuance frequency requirements • Defined offline CA • Incorporated OCSP requirements, moved from Section 2 • Incorporated privacy information publication restrictions, moved from Section 9	No negative impact

Section 5 • Clarified “remote workstation” practice note • Require delegated OCSP signing • Added requirement that any compromised CA must request revocation from any superior or cross certified CA	No negative impact
Section 6 • Removed references to SHA-1 • Updated cryptographic module requirements (require FIPS 140-2 Level 3 protection of CA signing keys) • Incorporated draft "Update Common Policy on use of CA signing Keys" Change Proposal submitted by Treasury • Reduce OCSP certificate validity from 3 years to 120 days • Require use of a VPN for remote workstation administration of CA	No negative impact Note: two affiliates require updates to OCSP certificate validity
Section 7 • Updated permitted key sizes (add RSA 4096 and EC P-384) and signing algorithms (sha384WithRSAEncryption, sha512WithRSAEncryption, and ecdsa-with-SHA512)	No negative impact
Section 8 • No major updates	No negative impact
Section 9 • No major updates	No negative impact

APPENDIX C: IMPACT OF CERTIFICATE PROFILE UPDATES

Profile Changes	CAs Impacted*
Authority Information Access & Certificate Revocation List Distribution Point - Require HTTP URI first	6
Authority Information Access - Allow .cer	No negative impact
DN Encoding: Allow only printableString and/or UTF8	No negative impact
Key Usage - Remove digital signature and non-repudiation bits from CA profiles • Removes ability to perform direct OCSP signing by a CA; delegated OCSP signing only	4 No CA operations currently impacted; possible future impact
Allow Subject Directory Attributes (e.g., citizenship)	No negative impact
Cross Certificate • Clarify appropriate use of requireExplicitPolicy and inhibitPolicyMapping, • Offer distinction from the Intermediate CA Certificate profile (new).	No negative impact
Intermediate Certificate (new profile) • Prohibit policy mappings • Policy constraints are optional • Subject Information Access extension is required, unless the CA certificate includes path length constraint of 0	No negative impact
OCSP Responder Certificate • EKU must be marked critical	11
Signature Certificates and Key Management Certificates • For PIV, id-kp-emailProtection must be included • rfc822Name is required if id-kp-emailProtection is asserted in Extended Key Usage	2

* based on Annual Review certificate samples

X.509 Certificate Policy

for the

U.S. Federal PKI

Common Policy Framework

Version 2.0

September 1~~.32~~

~~April 14~~, 2020

Signature Page

Co-chair, Federal Public Key Infrastructure Policy Authority DATE

Co-chair, Federal Public Key Infrastructure Policy Authority DATE

Revision History

Document Version	Document Date	Revision Details
1.0	May 7, 2007	Revised Common Policy (RFC 3647 format)
1.1	July 17, 2007	**2007-01**. Alignment of Cryptographic Algorithm Requirements with SP 800-78-1
1.2	September 12, 2007	**2007-02**. Requiring the inclusion of a subject DN in PIV Authentication Certificates
1.3	October 16, 2007	**2007-03**. Accommodating legacy PKIs for PIV Authentication
1.4	April 3, 2008	**2008-01.** § 8.3 Assessor's Relationship to Assessed Entity
1.5	November 20, 2008	**2008-02**. Include a provision for a role-based signature certificate
1.6	February 11, 2009	**2009-01.** nextUpdate in Certificate Revocation Lists (CRL) published by legacy Federal PKIs
1.7	April 15, 2009	**2009-02.** Allow the use of the PIV Authentication certificate as proof of identity and employment
1.8	January 21, 2010	**2010-01**. Align key length requirements w/ SP 800-57 **2010-02**. Remote Administration of Certification Authorities
1.9	March 15, 2010	**2010-03**. Allowing inclusion of UUIDs in Card Authentication Certificates
1.10	April 8, 2010	**2010-04**. § 8.1 & 8.4
1.11	August 16, 2010	**2010-05**. Clarify the archive definition and how its records are intended to be used

1.12	October 15, 2010	**2010-06.** Allow Federal Legacy PKIs to Directly Cross Certify with Common Policy CA
1.13	November 18, 2010	**2010-07**. Legacy use of SHA-1 during transition period Jan 1, 2011 to Dec 31, 2013
1.14	December 17, 2010	Clarify requirement to support CA Key Rollover
1.15	January 24, 2011	**2011-01**, CAs to assert policy OIDs in OCSP responder certificates for which the OCSP responder is authoritative
1.16	September 23, 2011	**2011-02**, Clarify requirements for device Subscribers and certificates
1.17	December 13, 2011	**2011-03**, Remove Requirements for LDAP References in Certificates
1.18	April 26, 2012	**2012-01.** Clarify RA audit requirements: revise Section 1.3.1.5, add new last sentence to first paragraph of Section 8, revise first paragraph of Section 8.1, revise Sections 8.4, 8.5, and 8.6, revise "Policy Management Authority (PMA)" glossary definition.
1.19	June 22, 2012	**2012-02.** Add new Section 4.1.1.4, *Code Signing Certificates*, to address change proposal (approved by FPKIPA on 6/12/12) requiring organizations receiving a code signing certificate to have access to a Time Stamp Authority.
1.20	August 19, 2012	**2012-03.** Add new language to Sections 3.2.3.2 and 9.6.3 to address change proposal (approved by FPKIPA on 8/14/12) to allow a human device sponsor, who is not physically located near the sponsored device, and/or who does not have sufficient administrative privileges on the sponsored device to fulfill these responsibilities, to delegate them to an authorized administrator of the device.

		2012-04. Revise Section 4.9.7 to address change proposal (approved by FPKIPA on 8/12/12) to detail and clarify the Common Policy CA's CRL issuance policies to ensure Offline Root CA operations are permitted.
1.21	December 18, 2012	**2012-05.** Revise Sections 1.2, 1.4.1, 3.1.1, 6.2.8, 6.3.2, 7.1.4, 7.1.6, and add new Sections 6.1.1.4 and 6.2.4.6 to address change proposal (approved by FPKIPA on 12/6/12) to create a new Common PIV Content Signing Policy OID.
1.22	December 2, 2013	**2013-01.** Clarify places in the Common Policy CP which were flagged during the FPKIMA Annual Audit as either contradictory with the FBCA CP or contradictory to current best practices. Clarify division of responsibilities between Trusted Roles (~~Section5~~Section 5.2.1); clarify meaning of "all Security Audit logs (Section 5.4.1), and allow audit logs to be removed from production site once reviewed (Section 5.4.3) **2013-02.** Remove SHA-1 policies from Common Policy.
1.23	May 5, 2014	**2013-03.** Require PIV Cards to be on the GSA Approved Products List (APL) Prior to Issuance and require annual PIV card testing.
1.24	May 7, 2015	**2015-01.** Create two new Common Derived PIV Authentication Certificate Policy OIDs in the Common Policy, and change/add text in appropriate sections throughout the CP.
1.25	September 22, 2016	**2016-01.** Alignment with CAB Forum Baseline Requirements (BR) v1.3.4. This will facilitate FPKI conformance to CAB Forum BRs for publicly-trusted SSL/TLS certificates, which will help promote inclusion of the Federal Root in public trust

		stores and provide guidance for issuance of publicly-trusted device certificates. **2016-02.** Allow a long term CRL when a CA retires a key after performing a key changeover to align with the FPKI CPS.
1.26	February 2, 2017	**2016-03**. Remove or update references to obsoleted RFCs. Changes to Sections 1.3.1.7, 3.1.2, 3.1.4, 4.9.7, and 10.
1.27	June 29, 2017	**2017-01:** Align CP with current FPKIMA practice for CA certificates. **2017-02:** Require CAs to publish information pertaining to resolved incidents on their websites. **2017-03:** Require CAs to notify the FPKIPA whenever a change is made to their infrastructure **2017-04:** Clarifies the period of time PIV card stock can continue to be used once it has been removed from the GSA APL.
1.28	April 4, 2018	**2018-01:** Key Recovery for key management certificates issued under the COMMON Policy
1.29	May 10, 2018	**2018-02:** Add reference to Annual Review Requirements **2018-03**: Mandate specific EKUs in certificates issued after June 30, 2019 **2018-04**: Certificate revocation requirements for Transitive Closure after August 15, 2018 **2018-05:** Requirements for virtual implementations
1.30	October 4, 2018	**2018-06:** Incorporate "supervised remote identity proofing" and other new guidance as defined in NIST SP 800-63-3 effective as of October 4, 2018

1.31	February 8, 2019	**2018-07:** Remove the common-public-trusted-serverAuth certificate policy and associated requirements effective as of February 8, 2019 **2018-08:** Permit retention of private signing key(s) following CA termination effective as of February 8, 2019
1.32	April 14, 2020	**2020-01:** Add support for federally issued Personal Identity Verification-Interoperable (PIV-I) credentials

~~FOREWORD~~

~~This is the policy framework governing the public key infrastructure (PKI) component of the Federal Enterprise Architecture. The policy framework incorporates multiple specific certificate policies: a policy for users with software cryptographic modules, a policy for users with hardware cryptographic modules, a policy for devices that sign Personal Identity Verification (PIV) data objects, a policy for devices with software cryptographic modules, a policy for devices with hardware cryptographic modules, a high assurance user policy, three user authentication policies, and a card authentication policy. There is one Certification Authority (CA) associated with the Common Policy Framework: The Federal Common Policy Root CA.~~

~~The user policies apply to Federal employees, contractors, and other affiliated personnel requiring PKI credentials for access to Federal systems that have not been designated by law as national security systems. The device policies apply to hardware devices and software applications operated by or on behalf of federal agencies. These policies may be used by PKIs whose certification practice statement (CPS) and compliance audit have been approved by the Federal PKI Policy Authority (FPKIPA). Such PKIs may be agency operated or may be operated by approved providers.~~

~~This policy framework supports hierarchical PKI, mesh PKI, and single CA implementations of this certificate policy. As such, constraints are established for the secure distribution of self-signed certificates for use as trust anchors. These constraints apply only to CAs that choose to distribute self-signed certificates.~~

~~This policy framework requires the use of FIPS 140 validated cryptographic modules by Federal employees, contractors, other affiliated personnel and devices for all cryptographic operations and the protection of trusted public keys. Software and hardware cryptographic mechanisms are equally acceptable under this policy framework. The policies for users with hardware cryptographic modules mandate Level 2 validation.~~

~~For entities associated with the Federal Common Policy Root CA, this policy framework requires the use of either 2048 bit RSA keys or 256 bit elliptic curve keys along with the SHA-256 and SHA-384 hash algorithms. CAs are required to use 2048 bit RSA keys or 256 bit elliptic curve keys when signing certificates and CRLs that expire on or after December 31, 2010. CAs are required to use SHA-256 or SHA-384 when signing certificates that are issued after December 31, 2010. All subscriber signature keys in certificates that expire on or after December 31, 2008 must be at least 2048 bit RSA keys or 256 bit elliptic curve keys. Subscriber authentication keys in certificates that expire on or after December 31, 2013 must be at least 2048 bit RSA keys or 256 bit elliptic curve keys.~~

~~The certificate policies that comprise this policy framework are consistent with RFC 3647, the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) Certificate Policy and Certification Practices Framework.~~

~~The terms and provisions of these certificate policies shall be interpreted under and governed by applicable Federal law.~~

2.0	September 1, 2020	**2020-02:** Consolidated update to Common Policy and associated profiles, effective as of September 1, 2021. See the change proposal cover sheet for more detail.

Table of Contents

~~1. Introduction .... 1~~

~~1.1 Overview 2~~

~~1.1.1 Certificate Policy (CP) 2~~

~~1.1.2 Relationship between the CP and the CPS 2~~

~~1.1.3 Scope 2~~

~~1.1.4 Interoperation with CAs Issuing under Different Policies 2~~

~~1.2 Document Name and Identification 2~~

~~1.3 PKI Participants 4~~

~~1.3.1 PKI Authorities 4~~

~~1.3.1.1 Federal Chief Information Officers Council .... 4~~

~~1.3.1.2 Federal PKI Policy Authority (FPKIPA) .... 4~~

~~1.3.1.3 FPKI Management Authority (FPKIMA) .... 4~~

~~1.3.1.4 FPKI Management Authority Program Manager .... 4~~

~~1.3.1.5 Policy Management Authority .... 5~~

~~1.3.1.6 Certification Authority .... 5~~

~~1.3.1.7 Certificate Status Servers .... 5~~

~~1.3.2 Registration Authorities 6~~

~~1.3.3 Trusted Agents 6~~

~~1.3.4 Subscribers 6~~

~~1.3.5 Relying Parties 7~~

~~1.3.6 Other Participants 7~~

~~1.4 Certificate Usage 7~~

~~1.4.1 Appropriate Certificate Uses 7~~

~~1.4.2 Prohibited Certificate Uses 8~~

~~1.5 Policy Administration 8~~

~~1.5.1 Organization Administering the Document 8~~

~~1.5.2 Contact Person 8~~

~~1.5.3 Person Determining CPS Suitability for the Policy 8~~

~~1.5.4 CPS Approval Procedures 8~~

~~1.6 Definitions and Acronyms 8~~

~~2. Publication and Repository Responsibilities .... 9~~

~~2.1 Repositories 9~~

~~2.2 Publication of Certification Information 9~~

~~2.2.1 Publication of Certificates and Certificate Status 9~~

~~2.2.2 Publication of CA Information 9~~

~~2.2.3 Interoperability 9~~

~~2.3 Time or Frequency of Publication 9~~

~~2.4 Access Controls on Repositories 10~~

~~3. Identification and Authentication ..... 11~~

~~3.1 Naming 11~~

~~3.1.1 Types of Names 11~~

~~3.1.2 Need for Names to Be Meaningful 16~~

~~3.1.3 Anonymity or Pseudonymity of Subscribers 16~~

~~3.1.4 Rules for Interpreting Various Name Forms 17~~

~~3.1.5 Uniqueness of Names 17~~

~~3.1.6 Recognition, Authentication, and Role of Trademarks 17~~

~~3.2 Initial Identity Validation 17~~

~~3.2.1 Method to Prove Possession of Private Key 17~~

~~3.2.2 Authentication of Organization Identity 17~~

~~3.2.3 Authentication of Individual Identity 18~~

~~3.2.3.1 Authentication of Human Subscribers ..... 18~~

~~3.2.3.2 Authentication of Devices ..... 20~~

~~3.2.3.3 Authentication for Derived PIV Credentials ..... 21~~

~~3.2.4 Non-verified Subscriber Information 22~~

~~3.2.5 Validation of Authority 22~~

~~3.2.6 Criteria for Interoperation 22~~

~~3.3 Identification and Authentication for Re-key Requests 22~~

~~3.3.1 Identification and Authentication for Routine Re-key 22~~

~~3.3.2 Identification and Authentication for Re-key after Revocation 23~~

~~3.4 Identification and Authentication for Revocation Request 23~~

~~4. Certificate Life-Cycle Operational Requirements ..... 24~~

~~4.1 Certificate Application 24~~

~~4.1.1 Who Can Submit a Certificate Application 24~~

~~4.1.1.1 CA Certificates ..... 24~~

~~4.1.1.2 User Certificates ..... 24~~

~~4.1.1.3 Device Certificates ..... 24~~

~~4.1.1.4 Code Signing Certificates ..... 24~~

~~4.1.2 Enrollment Process and Responsibilities 24~~
~~4.2 Certificate Application Processing 25~~
~~4.2.1 Performing Identification and Authentication Functions 25~~
~~4.2.2 Approval or Rejection of Certificate Applications 25~~
~~4.2.3 Time to Process Certificate Applications 25~~
~~4.3 Certificate Issuance 25~~
~~4.3.1 CA Actions During Certificate Issuance 25~~
~~4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 26~~
~~4.4 Certificate Acceptance 26~~
~~4.4.1 Conduct Constituting Certificate Acceptance26~~
~~4.4.2 Publication of the Certificate by the CA 26~~
~~4.4.3 Notification of Certificate Issuance by the CA to Other Entities 26~~
~~4.5 Key Pair and Certificate Usage 26~~
~~4.5.1 Subscriber Private Key and Certificate Usage 26~~
~~4.5.2 Relying Party Public key and Certificate Usage 26~~
~~4.6 Certificate Renewal 27~~
~~4.6.1 Circumstance for Certificate Renewal 27~~
~~4.6.2 Who May Request Renewal 27~~
~~4.6.3 Processing Certificate Renewal Requests 27~~
~~4.6.4 Notification of New Certificate Issuance to Subscriber 27~~
~~4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 27~~
~~4.6.6 Publication of the Renewal Certificate by the CA 27~~
~~4.6.7 Notification of Certificate Issuance by the CA to Other Entities 28~~
~~4.7 Certificate Re-key 28~~
~~4.7.1 Circumstance for Certificate Re-key 28~~
~~4.7.2 Who May Request Certification of a New Public Key 28~~
~~4.7.3 Processing Certificate Re-keying Requests 28~~
~~4.7.4 Notification of New Certificate Issuance to Subscriber 28~~
~~4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate 28~~
~~4.7.6 Publication of the Re-keyed Certificate by the CA 29~~
~~4.7.7 Notification of Certificate Issuance by the CA to Other Entities 29~~
~~4.8 Certificate Modification 29~~
~~4.8.1 Circumstance for Certificate Modification 29~~
~~4.8.2 Who May Request Certificate Modification 29~~

~~4.8.3 Processing Certificate Modification Requests 29~~
~~4.8.4 Notification of New Certificate Issuance to Subscriber 29~~
~~4.8.5 Conduct Constituting Acceptance of Modified Certificate 30~~
~~4.8.6 Publication of the Modified Certificate by the CA 30~~
~~4.8.7 Notification of Certificate Issuance by the CA to Other Entities 30~~
~~4.9 Certificate Revocation and Suspension 30~~
~~4.9.1 Circumstances for Revocation 30~~
~~4.9.2 Who Can Request Revocation 31~~
~~4.9.3 Procedure for Revocation Request 31~~
~~4.9.4 Revocation Request Grace Period 32~~
~~4.9.5 Time within which CA must Process the Revocation Request 32~~
~~4.9.6 Revocation Checking Requirements for Relying Parties 32~~
~~4.9.7 CRL Issuance Frequency 32~~
~~4.9.8 Maximum Latency for CRLs 33~~
~~4.9.9 On-line Revocation/Status Checking Availability 33~~
~~4.9.10 On-line Revocation Checking Requirements 34~~
~~4.9.11 Other Forms of Revocation Advertisements Available 34~~
~~4.9.12 Special Requirements Related To Key Compromise 34~~
~~4.9.13 Circumstances for Suspension 34~~
~~4.9.14 Who Can Request Suspension 34~~
~~4.9.15 Procedure for Suspension Request 34~~
~~4.9.16 Limits on Suspension Period 34~~
~~4.10 Certificate Status Services 34~~
~~4.10.1 Operational Characteristics 34~~
~~4.10.2 Service Availability 35~~
~~4.10.3 Optional Features 35~~
~~4.11 End Of Subscription 35~~
~~4.12 Key Escrow and Recovery 35~~
~~4.12.1 Key Escrow and Recovery Policy and Practices 35~~
~~4.12.2 Session Key Encapsulation and Recovery Policy and Practices 35~~
~~5. Facility, Management, and Operational Controls .... 36~~
~~5.1 Physical Controls 36~~
~~5.1.1 Site Location and Construction 36~~
~~5.1.2 Physical Access 36~~

~~5.1.2.1 Physical Access for CA Equipment .... 36~~
~~5.1.2.2 Physical Access for RA Equipment .... 37~~
~~5.1.2.3 Physical Access for CSS Equipment .... 37~~
~~5.1.3 Power and Air Conditioning 37~~
~~5.1.4 Water Exposures 37~~
~~5.1.5 Fire Prevention and Protection 37~~
~~5.1.6 Media Storage 37~~
~~5.1.7 Waste Disposal 38~~
~~5.1.8 Off-Site Backup 38~~
~~5.2 Procedural Controls 38~~
~~5.2.1 Trusted Roles 38~~
~~5.2.2 Number of Persons Required per Task 39~~
~~5.2.3 Identification and Authentication for Each Role 39~~
~~5.2.4 Roles Requiring Separation of Duties39~~
~~5.3 Personnel Controls 39~~
~~5.3.1 Qualifications, Experience, and Clearance Requirements 39~~
~~5.3.2 Background Check Procedures 39~~
~~5.3.3 Training Requirements 40~~
~~5.3.4 Retraining Frequency and Requirements 40~~
~~5.3.5 Job Rotation Frequency and Sequence 40~~
~~5.3.6 Sanctions for Unauthorized Actions 40~~
~~5.3.7 Independent Contractor Requirements 40~~
~~5.3.8 Documentation Supplied to Personnel 41~~
~~5.4 Audit Logging Procedures 41~~
~~5.4.1 Types of Events Recorded 41~~
~~5.4.2 Frequency of Processing Log 44~~
~~5.4.3 Retention Period for Audit Log 45~~
~~5.4.4 Protection of Audit Log 45~~
~~5.4.5 Audit Log Backup Procedures 45~~
~~5.4.6 Audit Collection System (Internal vs. External) 45~~
~~5.4.7 Notification to Event-Causing Subject 45~~
~~5.4.8 Vulnerability Assessments 45~~
~~5.5 Records Archival 46~~
~~5.5.1 Types of Events Archived 46~~

~~5.5.2 Retention Period for Archive 47~~
~~5.5.3 Protection of Archive 47~~
~~5.5.4 Archive Backup Procedures 48~~
~~5.5.5 Requirements for Time-Stamping of Records 48~~
~~5.5.6 Archive Collection System (Internal or External) 48~~
~~5.5.7 Procedures to Obtain and Verify Archive Information 48~~
~~5.6 Key Changeover 48~~
~~5.7 Compromise and Disaster Recovery 49~~
~~5.7.1 Incident and Compromise Handling Procedures 49~~
~~5.7.2 Computing Resources, Software, and/or Data Are Corrupted 49~~
~~5.7.3 Entity (CA) Private Key Compromise Procedures 50~~
~~5.7.4 Business Continuity Capabilities after a Disaster 50~~
~~5.8 CA or RA Termination 51~~
~~6. Technical Security Controls .... 52~~
~~6.1 Key Pair Generation and Installation 52~~
~~6.1.1 Key Pair Generation 52~~
~~6.1.1.1 CA Key Pair Generation .... 52~~
~~6.1.1.2 Subscriber Key Pair Generation .... 52~~
~~6.1.1.3 CSS Key Pair Generation .... 53~~
~~6.1.1.4 PIV Content Signing Key Pair Generation .... 53~~
~~6.1.2 Private Key Delivery to Subscriber 53~~
~~6.1.3 Public Key Delivery to Certificate Issuer 54~~
~~6.1.4 CA Public Key Delivery to Relying Parties 54~~
~~6.1.5 Key Sizes 55~~
~~6.1.6 Public Key Parameters Generation and Quality Checking 56~~
~~6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field) 56~~
~~6.2 Private Key Protection and Cryptographic Module Engineering Controls 57~~
~~6.2.1 Cryptographic Module Standards and Controls 57~~
~~6.2.2 Private Key (n out of m) Multi-Person Control 58~~
~~6.2.3 Private Key Escrow 59~~
~~6.2.4 Private Key Backup 59~~
~~6.2.4.1 Backup of CA Private Signature Key .... 59~~
~~6.2.4.2 Backup of Subscriber Private Signature Key .... 59~~
~~6.2.4.3 Backup of Subscriber Private Key Management Key .... 59~~

~~6.2.4.4 Backup of CSS Private Key .... 59~~

~~6.2.4.5 Backup of Device Private Keys .... 59~~

~~6.2.4.6 Backup of Common PIV Content Signing Key .... 59~~

~~6.2.5 Private Key Archival 60~~

~~6.2.6 Private Key Transfer into or from a Cryptographic Module 60~~

~~6.2.7 Private Key Storage on Cryptographic Module 60~~

~~6.2.8 Method of Activating Private Key 60~~

~~6.2.9 Method of Deactivating Private Key 61~~

~~6.2.10 Method of Destroying Private Key 61~~

~~6.2.11 Cryptographic Module Rating 61~~

~~6.3 Other Aspects of Key Pair Management 61~~

~~6.3.1 Public Key Archival 61~~

~~6.3.2 Certificate Operational Periods and Key Usage Periods 61~~

~~6.4 Activation Data 62~~

~~6.4.1 Activation Data Generation and Installation 62~~

~~6.4.2 Activation Data Protection 62~~

~~6.4.3 Other Aspects of Activation Data 62~~

~~6.5 Computer Security Controls 62~~

~~6.5.1 Specific Computer Security Technical Requirements 62~~

~~6.5.2 Computer Security Rating 64~~

~~6.6 Life Cycle Technical Controls 64~~

~~6.6.1 System Development Controls 64~~

~~6.6.2 Security Management Controls 65~~

~~6.6.3 Life Cycle Security Controls 65~~

~~6.7 Network Security Controls 65~~

~~6.8 Time-Stamping 66~~

~~7. Certificate, CRL, and OCSP Profiles .... 67~~

~~7.1 Certificate Profile 67~~

~~7.1.1 Version Number(s) 67~~

~~7.1.2 Certificate Extensions 67~~

~~7.1.3 Algorithm Object Identifiers 67~~

~~7.1.4 Name Forms 68~~

~~7.1.5 Name Constraints 68~~

~~7.1.6 Certificate Policy Object Identifier 68~~

~~7.1.7 Usage of Policy Constraints Extension 69~~

~~7.1.8 Policy Qualifiers Syntax and Semantics 69~~

~~7.1.9 Processing Semantics for the Critical Certificate Policies Extension69~~

~~7.1.10 Inhibit Any Policy Extension 69~~

~~7.2 CRL Profile 69~~

~~7.2.1 Version Number(s) 69~~

~~7.2.2 CRL and CRL Entry Extensions 70~~

~~7.3 OCSP Profile 70~~

~~7.3.1 Version Number(s) 70~~

~~7.3.2 OCSP Extensions 70~~

~~8. Compliance Audit and Other Assessments .... 71~~

~~8.1 Frequency or Circumstances of Assessment 71~~

~~8.2 Identity/Qualifications of Assessor 71~~

~~8.3 Assessor's Relationship to Assessed Entity 71~~

~~8.4 Topics Covered by Assessment 71~~

~~8.5 Actions Taken as a Result of Deficiency 72~~

~~8.6 Communication of Results 72~~

~~9. Other Business and Legal Matters .... 73~~

~~9.1 Fees 73~~

~~9.1.1 Certificate Issuance or Renewal Fees 73~~

~~9.1.2 Certificate Access Fees 73~~

~~9.1.3 Revocation or Status Information Access Fees 73~~

~~9.1.4 Fees for other Services 73~~

~~9.1.5 Refund Policy 73~~

~~9.2 Financial Responsibility 73~~

~~9.2.1 Insurance Coverage 73~~

~~9.2.2 Other Assets 73~~

~~9.2.3 Insurance or Warranty Coverage for End-Entities 73~~

~~9.3 Confidentiality of Business Information 73~~

~~9.3.1 Scope of Confidential Information 73~~

~~9.3.2 Information not within the Scope of Confidential Information 74~~

~~9.3.3 Responsibility to Protect Confidential Information 74~~

~~9.4 Privacy of Personal Information 74~~

~~9.4.1 Privacy Plan 74~~

~~9.4.2 Information Treated as Private 74~~
~~9.4.3 Information not Deemed Private 74~~
~~9.4.4 Responsibility to Protect Private Information74~~
~~9.4.5 Notice and Consent to Use Private Information 75~~
~~9.4.6 Disclosure Pursuant to Judicial or Administrative Process 75~~
~~9.4.7 Other Information Disclosure Circumstances75~~
~~9.5 Intellectual Property Rights 75~~
~~9.6 Representations and Warranties 75~~
~~9.6.1 CA Representations and Warranties 76~~
~~9.6.2 RA Representations and Warranties 76~~
~~9.6.3 Subscriber Representations and Warranties 76~~
~~9.6.4 Relying Parties Representations and Warranties 77~~
~~9.6.5 Representations and Warranties of Other Participants 77~~
~~9.7 Disclaimers of Warranties 77~~
~~9.8 Limitations of Liability 77~~
~~9.9 Indemnities 77~~
~~9.10 Term and Termination 78~~
~~9.10.1 Term 78~~
~~9.10.2 Termination 78~~
~~9.10.3 Effect of Termination and Survival 78~~
~~9.11 Individual Notices and Communications with Participants 78~~
~~9.12 Amendments 78~~
~~9.12.1 Procedure for Amendment 78~~
~~9.12.2 Notification Mechanism and Period 78~~
~~9.12.3 Circumstances under which OID must be Changed 78~~
~~9.13 Dispute Resolution Provisions 79~~
~~9.14 Governing Law 79~~
~~9.15 Compliance with Applicable Law 79~~
~~9.16 Miscellaneous Provisions 79~~
~~9.16.1 Entire Agreement 79~~
~~9.16.2 Assignment 79~~
~~9.16.3 Severability 79~~
~~9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights) 79~~
~~9.16.5 Force Majeure 79~~

~~9.17 Other Provisions 79~~

~~10. Bibliography .... 80~~

~~11. Acronyms and Abbreviations .... 84~~

~~12. Glossary .... 87~~

~~13. Acknowledgments.......... 97~~

~~Appendix A PIV and Common PIV Interoperable (Common PIV-I) Comparison.......... 98~~

1. Introduction 11~~16~~

1.1 Overview 12~~17~~

1.1.1 Certificate Policy (CP) 12~~17~~

1.1.2 Relationship between the CP and the CPS 12~~17~~

1.1.3 Scope 13~~17~~

1.1.4 Interoperation with CAs Issuing under Different Policies 13~~17~~

1.2 Document Name and Identification 13~~18~~

1.3 PKI Participants 16~~20~~

1.3.1 PKI Authorities 16~~20~~

1.3.1.1 Federal Chief Information Officers Council 16~~20~~

1.3.1.2 Federal PKI Policy Authority (FPKIPA) 17~~20~~

1.3.1.3 FPKI Management Authority (FPKIMA) 17~~21~~

1.3.1.4 FPKI Management Authority Program Manager 17~~21~~

1.3.1.5 Policy Management Authority (PMA) 17~~21~~

1.3.2 Certification Authorities 18~~21~~

1.3.3 Registration Authorities 18~~22~~

1.3.4 Subscribers 19~~22~~

1.3.5 Relying Parties 20~~23~~

1.3.6 Other Participants 20~~23~~

1.4 Certificate Usage 20~~23~~

1.4.1 Appropriate Certificate Uses 20~~23~~

1.4.2 Prohibited Certificate Uses 21~~23~~

1.5 Policy Administration 21~~24~~

1.5.1 Organization Administering the Document 21~~24~~

1.5.2 Contact Person 21~~24~~

1.5.3 Person Determining CPS Suitability for the Policy 21~~24~~

1.5.4 CPS Approval Procedures 21~~24~~

1.6 Definitions and Acronyms 22~~24~~

2. Publication and Repository Responsibilities 22~~24~~

2.1 Repositories 22~~24~~

2.2 Publication of Certification Information 22~~24~~

2.2.1 Publication of Certificates and Certificate Status 22~~24~~

2.2.2 Publication of CA Information 23~~25~~

2.3 Time or Frequency of Publication 24~~25~~

2.4 Access Controls on Repositories 24~~26~~

3. Identification and Authentication 24~~26~~

3.1 Naming 24~~26~~

3.1.1 Types of Names 24~~26~~

3.1.1.1 Subject Names 24~~26~~

3.1.1.2 Subject Alternative Names 29

3.1.2 Need for Names to Be Meaningful 32~~30~~

3.1.3 Anonymity or Pseudonymity of Subscribers 32~~30~~

3.1.4 Rules for Interpreting Various Name Forms 33~~30~~

3.1.5 Uniqueness of Names 33~~31~~

3.1.6 Recognition, Authentication, and Role of Trademarks 33~~31~~

3.2 Initial Identity Validation 33~~31~~

3.2.1 Method to Prove Possession of Private Key 33~~31~~

3.2.2 Authentication of Organization Identity 34~~31~~

3.2.3 Authentication of Individual Identity 34~~31~~

3.2.3.1 Authentication of Human Subscribers 34~~31~~

3.2.3.2 Authentication of Devices 38~~35~~

3.2.4 Non-verified Subscriber Information 39~~35~~

3.2.5 Validation of Authority 39~~36~~

3.2.6 Criteria for Interoperation 40~~36~~

3.3 Identification and Authentication for Re-key Requests 40~~36~~

3.3.1 Identification and Authentication for Routine Re-key 40~~36~~

3.3.2 Identification and Authentication for Re-key after Revocation 41~~37~~

3.4 Identification and Authentication for Revocation Request 41~~37~~

4. Certificate Life-Cycle Operational Requirements 41~~37~~

4.1 Certificate Application 41~~37~~

4.1.1 Who Can Submit a Certificate Application 42~~37~~

4.1.2 Enrollment Process and Responsibilities 42~~38~~

4.2 Certificate Application Processing 43~~38~~

4.2.1 Performing Identification and Authentication Functions 43~~38~~

4.2.2 Approval or Rejection of Certificate Applications 43~~38~~

4.2.3 Time to Process Certificate Applications 43~~38~~

4.3 Certificate Issuance 43~~39~~

4.3.1 CA Actions During Certificate Issuance 43~~39~~

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 44~~39~~

4.4 Certificate Acceptance 44~~39~~

4.4.1 Conduct Constituting Certificate Acceptance 44~~39~~

4.4.2 Publication of the Certificate by the CA 44~~39~~

4.4.3 Notification of Certificate Issuance by the CA to Other Entities 44~~40~~

4.5 Key Pair and Certificate Usage 45~~40~~

4.5.1 Subscriber Private Key and Certificate Usage 45~~40~~

4.5.2 Relying Party Public key and Certificate Usage 45~~40~~

4.6 Certificate Renewal 45~~40~~

4.6.1 Circumstance for Certificate Renewal 45~~40~~

4.6.2 Who May Request Renewal 45~~40~~

4.6.3 Processing Certificate Renewal Requests 46~~41~~

4.6.4 Notification of New Certificate Issuance to Subscriber 46~~41~~

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 46~~41~~

4.6.6 Publication of the Renewal Certificate by the CA 46~~41~~

4.6.7 Notification of Certificate Issuance by the CA to Other Entities 46~~41~~

4.7 Certificate Re-key 46~~41~~

4.7.1 Circumstance for Certificate Re-key 47~~41~~

4.7.2 Who May Request Certification of a New Public Key 47~~41~~

4.7.3 Processing Certificate Re-keying Requests 47~~42~~

4.7.4 Notification of New Certificate Issuance to Subscriber 47~~42~~

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate 47~~42~~

4.7.6 Publication of the Re-keyed Certificate by the CA 47~~42~~

4.7.7 Notification of Certificate Issuance by the CA to Other Entities 48~~42~~

4.8 Certificate Modification 48~~42~~

4.8.1 Circumstance for Certificate Modification 48~~42~~

4.8.2 Who May Request Certificate Modification 48~~42~~

4.8.3 Processing Certificate Modification Requests 48~~43~~

4.8.4 Notification of New Certificate Issuance to Subscriber 49~~43~~

4.8.5 Conduct Constituting Acceptance of Modified Certificate 49~~43~~

4.8.6 Publication of the Modified Certificate by the CA 49~~43~~

4.8.7 Notification of Certificate Issuance by the CA to Other Entities 49~~43~~

4.9 Certificate Revocation and Suspension 49~~43~~

4.9.1 Circumstances for Revocation 50~~44~~

4.9.2 Who Can Request Revocation 50~~44~~

4.9.3 Procedure for Revocation Request 51~~45~~

4.9.4 Revocation Request Grace Period 51~~45~~

4.9.5 Time within which CA must Process the Revocation Request 51~~45~~

4.9.6 Revocation Checking Requirements for Relying Parties 52~~45~~

4.9.7 CRL Issuance Frequency 52~~46~~

4.9.8 Maximum Latency for CRLs 53~~46~~

4.9.9 On-line Revocation/Status Checking Availability 54~~47~~

4.9.10 On-line Revocation Checking Requirements 54~~47~~

4.9.11 Other Forms of Revocation Advertisements Available 54~~47~~

4.9.12 Special Requirements Related To Key Compromise 55~~47~~

4.9.13 Circumstances for Suspension 55~~47~~

4.9.14 Who Can Request Suspension 55~~48~~

4.9.15 Procedure for Suspension Request 55~~48~~

4.9.16 Limits on Suspension Period 55~~48~~

4.10 Certificate Status Services 55~~48~~

4.10.1 Operational Characteristics 55~~48~~

4.10.2 Service Availability 55~~48~~

4.10.3 Optional Features 56~~48~~

4.11 End Of Subscription 56~~48~~

4.12 Key Escrow and Recovery 56~~48~~

4.12.1 Key Escrow and Recovery Policy and Practices 56~~48~~

4.12.2 Session Key Encapsulation and Recovery Policy and Practices 56~~48~~

5. Facility, Management, and Operational Controls 56~~49~~

5.1 Physical Controls 56~~49~~

5.1.1 Site Location and Construction 57~~49~~

5.1.2 Physical Access 57~~49~~

5.1.2.1 Physical Access for CA Equipment 57~~49~~

5.1.2.2 Physical Access for RA Equipment 58~~50~~

5.1.2.3 Physical Access for CSS Equipment 58~~50~~

5.1.3 Power and Air Conditioning 58~~50~~

5.1.4 Water Exposures 58~~50~~

5.1.5 Fire Prevention and Protection 58~~51~~

5.1.6 Media Storage 58~~51~~

5.1.7 Waste Disposal 58~~51~~
5.1.8 Off-Site Backup 59~~51~~
5.2 Procedural Controls 59~~51~~
5.2.1 Trusted Roles 59~~51~~
5.2.2 Number of Persons Required per Task 59~~52~~
5.2.3 Identification and Authentication for Each Role 60~~52~~
5.2.4 Roles Requiring Separation of Duties 60~~52~~
5.3 Personnel Controls 60~~52~~
5.3.1 Qualifications, Experience, and Clearance Requirements 60~~52~~
5.3.2 Background Check Procedures 60~~52~~
5.3.3 Training Requirements 61~~53~~
5.3.4 Retraining Frequency and Requirements 61~~53~~
5.3.5 Job Rotation Frequency and Sequence 61~~53~~
5.3.6 Sanctions for Unauthorized Actions 61~~53~~
5.3.7 Independent Contractor Requirements 61~~54~~
5.3.8 Documentation Supplied to Personnel 62~~54~~
5.4 Audit Logging Procedures 62~~54~~
5.4.1 Types of Events Recorded 62~~54~~
5.4.2 Frequency of Processing Log 65~~57~~
5.4.3 Retention Period for Audit Log 66~~58~~
5.4.4 Protection of Audit Log 66~~58~~
5.4.5 Audit Log Backup Procedures 66~~58~~
5.4.6 Audit Collection System (Internal vs. External) 66~~58~~
5.4.7 Notification to Event-Causing Subject 66~~58~~
5.4.8 Vulnerability Assessments 66~~58~~
5.5 Records Archival 67~~59~~
5.5.1 Types of Events Archived 67~~59~~
5.5.2 Retention Period for Archive 68~~60~~
5.5.3 Protection of Archive 68~~60~~
5.5.4 Archive Backup Procedures 69~~60~~
5.5.5 Requirements for Time-Stamping of Records 69~~60~~
5.5.6 Archive Collection System (Internal or External) 69~~60~~
5.5.7 Procedures to Obtain and Verify Archive Information 69~~61~~
5.6 Key Changeover 69~~61~~

5.7 Compromise and Disaster Recovery 70~~61~~
5.7.1 Incident and Compromise Handling Procedures 70~~61~~
5.7.2 Computing Resources, Software, and/or Data Are Corrupted 71~~62~~
5.7.3 Entity (CA) Private Key Compromise Procedures 71~~62~~
5.7.4 Business Continuity Capabilities after a Disaster 72~~63~~
5.8 CA Termination 72~~63~~
6. Technical Security Controls 73~~64~~
6.1 Key Pair Generation and Installation 73~~64~~
6.1.1 Key Pair Generation 73~~64~~
6.1.1.1 CA Key Pair Generation 73~~64~~
6.1.1.2 Subscriber Key Pair Generation 73~~64~~
6.1.1.3 CSS Key Pair Generation 74~~64~~
6.1.1.4 PIV Content Signing Key Pair Generation 74~~64~~
6.1.2 Private Key Delivery to Subscriber 74~~64~~
6.1.3 Public Key Delivery to Certificate Issuer 75~~65~~
6.1.4 CA Public Key Delivery to Relying Parties 75~~65~~
6.1.5 Key Sizes 76~~65~~
6.1.6 Public Key Parameters Generation and Quality Checking 78~~66~~
6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field) 78~~66~~
6.2 Private Key Protection and Cryptographic Module Engineering Controls 80~~67~~
6.2.1 Cryptographic Module Standards and Controls 80~~67~~
6.2.2 Private Key (n out of m) Multi-Person Control 82~~69~~
6.2.3 Private Key Escrow 82~~69~~
6.2.4 Private Key Backup 83~~69~~
6.2.5 Private Key Archival 84~~70~~
6.2.6 Private Key Transfer into or from a Cryptographic Module 85~~70~~
6.2.7 Private Key Storage on Cryptographic Module 85~~70~~
6.2.8 Method of Activating Private Key 85~~70~~
6.2.9 Method of Deactivating Private Key 87~~71~~
6.2.10 Method of Destroying Private Key 87~~72~~
6.2.11 Cryptographic Module Rating 87~~72~~
6.3 Other Aspects of Key Pair Management 87~~72~~
6.3.1 Public Key Archival 87~~72~~
6.3.2 Certificate Operational Periods and Key Usage Periods 87~~72~~

6.4 Activation Data 89~~73~~

6.4.1 Activation Data Generation and Installation 89~~73~~

6.4.2 Activation Data Protection 89~~73~~

6.4.3 Other Aspects of Activation Data 89~~73~~

6.5 Computer Security Controls 89~~74~~

6.5.1 Specific Computer Security Technical Requirements 89~~74~~

6.5.2 Computer Security Rating 91~~75~~

6.6 Life Cycle Technical Controls 91~~75~~

6.6.1 System Development Controls 91~~75~~

6.6.2 Security Management Controls 92~~75~~

6.6.3 Life Cycle Security Controls 92~~76~~

6.7 Network Security Controls 92~~76~~

6.8 Time-Stamping 93~~76~~

7. Certificate, CRL, and OCSP Profiles 93~~76~~

7.1 Certificate Profile 93~~76~~

7.1.1 Version Number(s) 93~~76~~

7.1.2 Certificate Extensions 93~~77~~

7.1.3 Algorithm Object Identifiers 94~~77~~

7.1.4 Name Forms 95~~78~~

7.1.5 Name Constraints 95~~78~~

7.1.6 Certificate Policy Object Identifier 96~~78~~

7.1.7 Usage of Policy Constraints Extension 96~~78~~

7.1.8 Policy Qualifiers Syntax and Semantics 97~~79~~

7.1.9 Processing Semantics for the Critical Certificate Policies Extension 97~~79~~

7.1.10 Inhibit Any Policy Extension 97~~79~~

7.2 CRL Profile 97~~79~~

7.2.1 Version Number(s) 97~~79~~

7.2.2 CRL and CRL Entry Extensions 97~~79~~

7.3 OCSP Profile 97~~79~~

7.3.1 Version Number(s) 97~~79~~

7.3.2 OCSP Extensions 97~~79~~

8. Compliance Audit and Other Assessments 98~~80~~

8.1 Frequency or Circumstances of Assessment 98~~80~~

8.2 Identity/Qualifications of Assessor 98~~80~~

8.3 Assessor’s Relationship to Assessed Entity 99~~80~~

8.4 Topics Covered by Assessment 99~~81~~

8.5 Actions Taken as a Result of Deficiency 99~~81~~

8.6 Communication of Results 100~~81~~

9. Other Business and Legal Matters 100~~82~~

9.1 Fees 100~~82~~

9.1.1 Certificate Issuance or Renewal Fees 100~~82~~

9.1.2 Certificate Access Fees 100~~82~~

9.1.3 Revocation or Status Information Access Fees 100~~82~~

9.1.4 Fees for other Services 100~~82~~

9.1.5 Refund Policy 100~~82~~

9.2 Financial Responsibility 101~~82~~

9.2.1 Insurance Coverage 101~~82~~

9.2.2 Other Assets 101~~82~~

9.2.3 Insurance or Warranty Coverage for End-Entities 101~~82~~

9.3 Confidentiality of Business Information 101~~82~~

9.3.1 Scope of Confidential Information 101~~82~~

9.3.2 Information not within the Scope of Confidential Information 101~~83~~

9.3.3 Responsibility to Protect Confidential Information 101~~83~~

9.4 Privacy of Personal Information 102~~83~~

9.4.1 Privacy Plan 102~~83~~

9.4.2 Information Treated as Private 102~~83~~

9.4.3 Information not Deemed Private 102~~83~~

9.4.4 Responsibility to Protect Private Information 102~~83~~

9.4.5 Notice and Consent to Use Private Information 102~~84~~

9.4.6 Disclosure Pursuant to Judicial or Administrative Process 103~~84~~

9.4.7 Other Information Disclosure Circumstances 103~~84~~

9.5 Intellectual Property Rights 103~~84~~

9.6 Representations and Warranties 103~~84~~

9.6.1 CA Representations and Warranties 103~~84~~

9.6.2 RA Representations and Warranties 104~~85~~

9.6.3 Subscriber Representations and Warranties 104~~85~~

9.6.4 Relying Parties Representations and Warranties 105~~86~~

9.6.5 Representations and Warranties of Other Participants 105~~86~~

9.7 Disclaimers of Warranties 105~~86~~
9.8 Limitations of Liability 105~~86~~
9.9 Indemnities 105~~86~~
9.10 Term and Termination 105~~86~~
9.10.1 Term 105~~86~~
9.10.2 Termination 105~~86~~
9.10.3 Effect of Termination and Survival 105~~86~~
9.11 Individual Notices and Communications with Participants 105~~86~~
9.12 Amendments 106~~87~~
9.12.1 Procedure for Amendment 106~~87~~
9.12.2 Notification Mechanism and Period 106~~87~~
9.12.3 Circumstances under which OID must be Changed 106~~87~~
9.13 Dispute Resolution Provisions 106~~87~~
9.14 Governing Law 106~~87~~
9.15 Compliance with Applicable Law 106~~87~~
9.16 Miscellaneous Provisions 107~~87~~
9.16.1 Entire Agreement 107~~87~~
9.16.2 Assignment 107~~88~~
9.16.3 Severability 107~~88~~
9.16.4 Enforcement (Attorneys’ Fees and Waiver of Rights) 107~~88~~
9.16.5 Force Majeure 107~~88~~
9.17 Other Provisions 107~~88~~
Appendix A: PIV and Common PIV Interoperable Comparison 109~~89~~
Appendix B: References 112~~91~~
Appendix C: Acronyms and Abbreviations 116~~94~~
Appendix D: Glossary 118~~96~~

1. Introduction

This certificate policy (CP) includes ~~many~~the following distinct certificate policies: ~~a~~

- Three Personal Identity Verification (PIV) authentication policies;
- A PIV Interoperable (PIV-I) authentication policy for ~~users~~use by federal agencies;
- A PIV Card Authentication policy;
- A PIV-I Card Authentication policy for use by federal agencies;
- A policy for devices that sign PIV data objects;
- A policy for federal devices that sign PIV-I data objects;
- A policy for Human Subscribers with software cryptographic modules~~,~~;
- A policy for ~~users~~Human Subscribers with hardware cryptographic modules~~,~~;
- A high assurance policy for Human Subscribers;
- A policy for devices with software cryptographic modules~~,~~; and
- A policy for devices with hardware cryptographic modules~~, a policy for devices that sign PIV data objects, a high assurance user policy, three user authentication policies, and a card authentication policy.~~ .

In this document, the term “device” means a non-person entity, i.e., a hardware device or software application. ~~Where a specific policy is not stated, the policies and procedures in this specification apply equally to all policies.~~

~~The use of SHA-1 to create digital signatures is not allowed under Common Policy after 12/31/2013.~~

~~The user~~Certificates intended for code signing are not covered by this policy.

Where a specific policy is not stated, the requirements in this specification apply equally to all policies.

The Human Subscriber policies apply to certificates issued to federal employees, contractors, and other affiliated personnel for the purposes of authentication, signature, and confidentiality. This CP was explicitly designed to support access to federal systems that have not been designated national security systems.

A ~~PKI~~Certification Authority (CA) that ~~uses~~operates in accordance with this CP will provide the following security management services:

- Key generation/storage
- Key escrow and recovery
- Certificate generation, modification, re-key, and distribution
- Certificate revocation list (CRL) generation and distribution
- ~~Directory~~Repository management of certificate related items
- Certificate token initialization/programming/management

- System management functions (e.g., security audit, configuration management, archive.)

~~The user policies require Federal employees, contractors, and other affiliated personnel to use FIPS 140 validated cryptographic modules for cryptographic operations and the protection of trusted public keys. The device policy also requires use of FIPS 140 validated cryptographic modules for cryptographic operations and the protection of trusted public keys.~~

~~This policy does not presume any particular PKI architecture. The policy may be implemented through a hierarchical PKI, mesh PKI, or a single certification authority (CA).~~ Any CA that asserts ~~this policy~~these policies in certificates must obtain prior approval from the Federal PKI Policy Authority~~. CAs~~; approval is dependent upon a Certification Practices Statement (CPS) that clearly describes how each requirement in this CP is fulfilled, or, for Federal agencies that operate their own PKI, a comparable CP. For any section of this policy containing no stipulation, the CPS must indicate whether it is applicable, and if so, describe the associated practices. CAs operated by federal agencies that issue certificates under this policy may operate simultaneously under other policies. ~~Such~~CAs that operate simultaneously under this policy and under other policies must assert at least one policy in all issued certificates. CAs must not assert the OIDs in this policy in certificates unless they are issued in accordance with all the requirements of this policy.

~~This policy establishes requirements for the secure distribution of self-signed certificates for use as trust anchors. These constraints apply only to CAs that chose to distribute self-signed certificates, such as a hierarchical PKI's root CA.~~

~~This CP is consistent with request for comments (RFC) 3647, the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) Certificate Policy and Certification Practices Framework.~~

The root Certification Authority (CA) associated with the Common Policy Framework is the Federal Common Policy CA, operated by the Federal PKI Management Authority (FPKIMA).

This CP follows the RFC 3647 framework.

1.1. Overview

1.1.1. Certificate Policy (CP)

~~Certificates issued under this policy contain a registered certificate policy object identifier (OID), which may be used by a relying party to decide whether a certificate is trusted for a particular purpose.~~ This CP applies only to CAs owned by or operated on behalf of the Federal Government that issue certificates according to this policy.

1.1.2. Relationship between the CP and the CPS

This CP states ~~what assurance can be placed in a certificate~~ the requirements for the issuance and management of certificates issued by the ~~CA.~~CAs, and requirements for the operation of the CAs. The Certification Practice Statement (CPS) states how the CA ~~establishes that~~

~~assurance.~~(s) implement the requirements. Each CA that issues certificates under this CP ~~shall~~must have a corresponding approved CPS.

1.1.3. Scope

The scope of this U.S. Federal PKI Common Policy Framework CP includes the Certification Authorities used for issuing and managing certificates that are valid to the Federal Common Policy CA on behalf of federal executive branch agencies. This CP applies to certificates issued to CAs, devices, and federal employees, contractors and other affiliated personnel. This CP does not ~~apply to~~include certificates issued to groups ~~of people~~or intended to be shared.

Federal Government departments and agencies operate CAs that are intended to issue certificates for only locally trusted purposes. These CAs do not have a certification path to the Federal Common Policy CA and should not assert the policy OIDs defined in this CP.

1.1.4. Interoperation with CAs Issuing under Different Policies

~~Except for legacy~~ Federal ~~PKIs, interoperation with~~Government agency CAs ~~that issue under different policies will be achieved through policy mapping and cross-certification through the Federal Bridge Certification Authority. Legacy Federal PKIs~~ may perform ~~policy mapping and~~ cross-certification with either the Federal Common Policy ~~Root~~ CA or Federal Bridge ~~Certification Authority~~CA at their discretion.

~~Note that~~ Interoperability may also be achieved through other means, such as trust lists~~, to meet local requirements~~.

1.2. Document Name and Identification

This ~~CP provides substantial assurance concerning identity of certificate subjects.~~ is the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework.

Certificates issued in accordance with this CP ~~and associated with the Federal Common Policy Root CA shall~~must assert at least one of the following OIDs in the certificate ~~policy~~policies extension:

~~Table 1 – id-fpki-common Policy OIDs~~

id-fpki-common-policy	::= {2 16 840 1 101 3 2 1 3 6}
id-fpki-common-hardware	::= {2 16 840 1 101 3 2 1 3 7}
id-fpki-common-devices	::= {2 16 840 1 101 3 2 1 3 8}
id-fpki-common-devicesHardware	::= {2 16 840 1 101 3 2 1 3 36}
id-fpki-common-authentication	::= {2 16 840 1 101 3 2 1 3 13}
id-fpki-common-high	::= {2 16 840 1 101 3 2 1 3 16}
id-fpki-common-cardAuth	::= {2 16 840 1 101 3 2 1 3 17}

id-fpki-common-piv-contentSigning	::= {2 16 840 1 101 3 2 1 3 39}
id-fpki-common-derived-pivAuth	::= {2 16 840 1 101 3 2 1 3 40}
id-fpki-common-derived-pivAuth-hardware	::= {2 16 840 1 101 3 2 1 3 41}
id-fpki-common-pivi-authentication	::= {2 16 840 1 101 3 2 1 3 45}
id-fpki-common-pivi-cardAuth	::= {2 16 840 1 101 3 2 1 3 46}
id-fpki-common-pivi-contentSigning	::= {2 16 840 1 101 3 2 1 3 47}

~~Certificates issued to CAs may contain a subset of these OIDs. Certificates issued to users, other than devices, to support digitally signed documents or key management may contain either id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-High. Subscriber certificates issued to devices under this policy that use FIPS 140 Level 2 or higher cryptographic modules shall include one or more of id-fpki-common-deviceHardware, or id-fpki-common-devices. Subscriber certificates issued to devices under this policy using software cryptographic modules shall include id-fpki-common-devices.~~

~~This document includes five policies specific to FIPS 201 Personal Identity Verification (PIV) of Federal Employees and Contractors. Certificates issued to users supporting authentication but not digital signature, where the corresponding private key is stored on a PIV Card, may contain id-fpki-common-authentication. Certificates issued to users supporting authentication where the private key is stored on a PIV Card and can be used without user authentication may contain id-fpki-common-cardAuth. Certificates issued to users, in accordance with NIST SP 800-157, supporting authentication, but not digital signature, where the corresponding private key is not stored on a PIV Card, may contain either id-fpki-common-derived-pivAuth-hardware or id-fpki-common-derived-pivAuth as appropriate. The id-fpki-common-piv-contentSigning policy shall only be asserted in certificates issued to devices that sign PIV data objects in accordance with [FIPS 201] or [SP 800-157].~~

~~Certificates issued to users supporting authentication where the private key is stored on a Common PIV-I credential and requires user authentication shall contain id-fpki-common-pivi-authentication. Certificates issued to users supporting authentication where the private key is stored on a Common PIV-I credential and can be used without user authentication shall contain id-fpki-common-pivi-cardAuth. The id-fpki-common-pivi-contentSigning policy shall only be asserted in certificates issued to devices that sign Common PIV-I credential data objects.~~

CA certificates may contain a subset of these OIDs.

Subscriber certificates must contain an appropriate policy OID as described in the following tables:

FIPS 201 Personal Identity Verification (PIV) Human Subscriber Certificates

Certificates asserting the following policies are issued to Human Subscribers and are limited to use with PIV credentials by FIPS 201.

PIV Authentication certificate with the private key on a PIV credential	id-fpki-common-authentication
Derived PIV Authentication certificate issued in accordance with NIST SP 800-157 where the private key is not on a PIV credential	id-fpki-common-derived-pivAuth-hardware or id-fpki-common-derived-pivAuth as appropriate

Additional Human Subscriber Certificates

Digital signature certificate with the private key on a PIV credential	id-fpki-common-hardware or id-fpki-common-high
Digital signature certificate with the private key not on a PIV credential	id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-high
Key Management certificate, whether or not on a PIV credential	id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-high
Common PIV-I Authentication certificate with the private key on a federally-issued PIV-I credential	id-fpki-common-pivi-authentication
Other authentication certificate	id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-high

The requirements associated with id-fpki-common-pivi-authentication ~~and id-fpki-common-pivi-cardAuth~~ are identical to id-fpki-common-authentication ~~and id-fpki-common-cardAuth, respectively~~, with the exception of the need for a National Agency Check with Inquiries (NACI) and associated favorable adjudication. See Appendix A for additional comparisons~~, see Appendix A~~ between PIV and Common PIV-I credentials.

FIPS 201 Personal Identity Verification (PIV) Device Subscriber Certificates

Certificates asserting the following policies are issued to Device Subscribers and are limited to use with PIV credentials by FIPS 201.

Card Authentication certificate with the private key on a PIV credential	id-fpki-common-cardAuth

Content Signing certificate used to sign PIV data objects in accordance with [FIPS 201] or [SP 800-157]	id-fpki-common-piv-contentSigning

The requirements associated with id-fpki-common-piv-contentSigning ~~and id-fpki-common-pivi-contentSigning~~ are identical to id-fpki-common-devicesHardware except where specifically noted in the text.

Additional Device Subscriber Certificates

Certificates asserting the following policies may be issued to devices or software systems.

FIPS 140 Level 2 or higher hardware cryptographic modules	id-fpki-common-deviceHardware
FIPS 140 Level 1 or higher cryptographic modules	id-fpki-common-devices
Common PIV-I Card Authentication certificate with the private key on a federally-issued PIV-I credential	id-fpki-common-pivi-cardAuth
Common PIV-I Content Signing certificate used to sign federally-issued PIV-I data objects in accordance with [SP 800-157]	id-fpki-common-pivi-contentSigning

The requirements associated with id-fpki-common-pivi-cardAuth are identical to id-fpki-common-cardAuth, with the exception of the need for a NACI and associated favorable adjudication.

The requirements associated with id-fpki-common-pivi-contentSigning and are identical to id-fpki-common-piv-contentSigning, except where specifically noted in the text.

1.3. PKI Participants

The following are roles relevant to the administration and operation of CAs under this policy:

1.3.1. PKI Authorities

1.3.1.1. Federal Chief Information Officers Council

The Federal Chief Information Officer (CIO) Council comprises the Chief Information Officers of all cabinet level departments and other independent agencies. The Federal CIO Council has established the framework for the interoperable Federal PKI (FPKI) and oversees the operation of the organizations responsible for governing and promoting its use. In particular, this CP was established under the authority ~~of~~ and ~~with the~~ approval of the Federal CIO Council.

1.3.1.2. Federal PKI Policy Authority (FPKIPA)

The Federal Public Key Infrastructure Policy Authority (FPKIPA) is a ~~group~~sub-council comprised of U.S. Federal Government ~~Agencies (including cabinet-level Departments)~~agency representatives and is chartered ~~by~~under the Federal Chief Information Security Officer (CISO) Council, under the Federal CIO Council. The FPKIPA owns this certificate policy and represents the interest of the Federal CIOs~~. ~~ and Federal CISOs.

The FPKIPA is responsible for:

- Maintaining this CP,
- Approving the CPS for each CA that issues certificates under this policy,
- Approving the compliance audit report for each CA issuing certificates under this policy, and
- Ensuring continued conformance of each CA that issues certificates under this policy with applicable requirements as a condition for allowing continued participation.

1.3.1.3. FPKI Management Authority (FPKIMA)

The FPKIMA is the ~~organization~~government program that operates and maintains the ~~Common Policy Root CAs~~Federal PKI operational environment on behalf of the U.S. Government~~, subject to the direction of the FPKIPA~~.

1.3.1.4. FPKI Management Authority Program Manager

The Program Manager is the individual within the FPKIMA who has principal responsibility for overseeing the ~~proper~~ operation of the Federal Common Policy ~~Root CAs~~CA, including the required repository, and selecting the FPKIMA staff. ~~The Program Manager is selected by the FPKIMA and reports to the FPKIPA. The FPKIMA Program Manager must hold a Top Secret~~For additional personnel security ~~clearance.~~controls associated with this role see Section 5.3.1.

1.3.1.5. Policy Management Authority (PMA)

~~Each~~ A PMA is an individual or group established by an organization ~~that provides PKI services under this policy shall identify an individual or group that is responsible for maintaining the Shared Service Provider's (SSP) CPS and for~~ or agency for the purpose of ensuring ~~that~~ all ~~SSP~~ PKI components ~~(e.g., CAs, CSSs, CMSs, RAs)~~ are operated in compliance with ~~the SSP~~an appropriate CPS and this CP. ~~This body is referred to as the SSP PMA within this CP. Agencies that contract for the services of~~ All organizations and agencies operating a ~~CA~~PKI under this policy~~, shall~~ must establish a ~~management body to manage any agency-operated components (e.g., RAs or repositories) and resolve name space collisions. This body shall be referred to as an Agency Policy Management Authority, or Agency PMA.~~

~~An SSP~~ PMA ~~shall be responsible for notifying its customer Agency PMAs and the FPKIPA of any change to the infrastructure that has the potential to affect the FPKI operational environment~~

~~at least two weeks prior to implementation; all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the change shall be provided to the FPKIPA within 24 hours following implementation.~~

~~An Agency~~. The PMA ~~is responsible for ensuring that all Agency operated PKI components (e.g., CAs, CSSs, CMSs, RAs) are operated in compliance with this CP and the applicable CPS and shall~~must identify an individual to serve as the liaison for that organization or agency to the FPKIPA~~ and the SSP PMA. ~~.

1.3.2. Certification ~~Authority~~Authorities

The CA is the collection of hardware, software and operating personnel that create, sign, and issue public key certificates to Subscribers. The CA is responsible for~~ the~~ issuing and managing certificates including:

- The certificate manufacturing process
- Publication of certificates
- Revocation of certificates
- Generation and destruction of CA signing keys
- Ensuring that all aspects of the CA services, operations, and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

~~*1.3.2.1. Certificate Status Servers*~~

~~PKIs may optionally include an authority that provides status information about certificates on behalf of a CA through on-line transactions. In particular, PKIs may include OCSP responders to provide on-line status information. Such an authority is termed a certificate status server (CSS). Where the CSS is identified in certificates as an authoritative source for revocation information, the operations of that authority are considered within the scope of this CP. A Certificate Status Server (CSS) shall assert all the policy OIDs for which it is authoritative. Examples include OCSP servers that are identified in the authority information access (AIA) extension. OCSP servers that are locally trusted, as described in [RFC 6960], are not covered by this policy.~~

1.3.3. Registration Authorities

~~The registration authorities (RAs)~~ A Registration Authority (RA) is an entity authorized by the CA to collect~~ and~~, verify~~ each subscriber's identity~~, and submit information provided by potential Subscribers for the purpose of issuing public key certificates. The term RA refers to hardware, software, and individuals that ~~is to be entered into the subscriber's public key certificate. The RA performs its~~may collectively perform this function. Individuals fulfilling the RA function are acting in ~~accordance with~~ a ~~CPS approved by the FPKIPA.~~Trusted Role. The RA is responsible for:

- Control over the registration process.
- The identification and authentication process.

~~1.3.4. Trusted Agents~~

~~The~~A Trusted Agent is a person who satisfies all the trustworthiness requirements for an RA and who performs identity proofing as a proxy for the RA. ~~The~~A Trusted Agent records information from and verifies biometrics (e.g., photographs) on presented credentials for Applicants who cannot appear in person at an RA. ~~The CPS will identify the parties responsible for providing such services, and the mechanisms for determining their trustworthiness.~~

~~1.3.5.~~1.3.4. Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate. ~~The subscriber asserts that he or she uses the key~~For this CP and ~~certificate in accordance with the certificate policy asserted in the certificate, and does not issue~~all certificates~~. For this policy~~ issued, Subscribers are limited to federal employees, contractors, affiliated personnel, and devices operated by or on behalf of federal agencies. ~~CAs are sometimes technically considered "subscribers" in a PKI. However,~~ The term "Subscriber" as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information. A Subscriber may be referred to as an "Applicant" after applying for a certificate, but before the certificate issuance procedure is completed.

There is a subset of Human Subscribers who will be issued role-based certificates. These certificates~~ will~~ identify a specific role on behalf of which the Subscriber is authorized to act rather than the Subscriber's name~~ and ~~. These certificates are issued in the interest of supporting accepted business practices. The role-based certificate can be used in situations where non-repudiation is desired. Normally, it will be issued in addition to an individual Subscriber certificate. A specific role may be identified in certificates issued to multiple Subscribers~~,~~; however, the key pair will be unique to each individual role-based certificate~~ (i.e.~~. For example, there may be four individuals ~~carrying~~with a certificate issued in the role of "Secretary of Commerce~~"~~". However, each of the four ~~individual~~ certificates will ~~carry~~have unique keys and certificate ~~identifiers).~~serial numbers. Roles for which role-based certificates may be issued are limited to those that are held by a unique individual within an organization (e.g. Chief Information Officer, GSA is a unique individual whereas Program Analyst, GSA is not).

~~Practice Note: When determining whether a role-based certificate is authorized, consider whether the role carries inherent authority beyond the job title. Role-based certificates may also be used for individuals on temporary assignment, where the temporary assignment carries an authority not shared by the individuals in their usual occupation, for example: "*Watch Commander, Task Force 1*".~~

Practice Note: When determining whether a role-based certificate is authorized, consider whether the role carries inherent authority beyond the job title. Role-based certificates may also be used for individuals on temporary assignment, where the temporary assignment carries an authority not shared by the individuals in their usual occupation, for example: "Watch Commander, Task Force 1".

~~1.3.6.~~1.3.5. Relying Parties

A relying party is the entity that relies on the validity of the binding of the Subscriber's ~~name~~identity to a public key. The relying party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The relying party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the ~~certificate.~~certificate's private key. A relying party may use information in the certificate (such as ~~CP~~certificate policy identifiers, key usage, or extended key usage) to determine ~~the suitability of the certificate for a particular use~~its appropriate usage.

For this certificate policy, the relying party may be any entity that wishes to validate the binding of a public key to the name ~~(or role) of a federal employee, contractor, or other affiliated personnel~~of a Subscriber.

~~1.3.7.~~1.3.6. Other Participants

The CAs and RAs operating under this CP may require the services of other security, community, and application authorities, such as compliance auditors~~ and attribute authorities. The CPS will identify the parties responsible for providing such services, and the mechanisms used to support these services.~~.

Participating agencies that do not operate a PKI directly must identify one or more Agency Points of Contact (POC) as liaisons to the issuing PKI and the FPKIPA.

1.4. CERTIFICATE USAGE

1.4.1. Appropriate Certificate Uses

~~The sensitivity of the information processed or protected using certificates issued by the CA will vary significantly. Organizations must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each organization for each application and is not controlled by this CP.~~

~~This CP is intended to support the use of validated public keys to access Federal systems that have not been designated national security systems. While a validated public key is not generally sufficient to grant access the key may be sufficient when supplemented by appropriate authorization mechanisms. Credentials~~Certificates issued under this CP may be used for authentication to Federal systems.

Certificates issued under this CP may also be used for key ~~establishment. ~~management, signature, and confidentiality requirements for Federal Government processes.

This policy is intended to support ~~applications~~use cases involving unclassified information, which can include sensitive unclassified data protected pursuant to federal statutes and regulations.

~~Credentials issued under the id-fpki-common-policy and id-fpki-common-derived-pivAuth policies are intended to meet the requirements for Level 3 authentication, as defined by the OMB~~

~~E-Authentication Guidance. [E-Auth] Credentials issued under the id-fpki-common-hardware, id-fpki-common-authentication, id-fpki-common-pivi-authentication, id-fpki-common-derived-pivAuth-hardware, and id-fpki-common-High policies meet the requirements for Level 4 authentication, as defined by the OMB E-Authentication Guidance. [E-Auth]~~

~~Credentials issued under the id-fpki-common-piv-contentSigning or id-fpki-common-pivi-contentSigning policy are intended to meet the requirements in FIPS 201 and SP 800-157 as the digital signatory of the PIV Card Holder Unique IDentifier (CHUID) and associated PIV data objects.~~

~~In addition, this policy may support signature and confidentiality requirements for Federal government processes.~~

Agencies make risk-informed decisions when using certificates to manage the identities of federal systems and users by evaluating the environment, associated threats, and vulnerabilities in determining the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by agencies for each application and is not controlled by this CP.

1.4.2. Prohibited Certificate Uses

Certificates that assert id-fpki-common-cardAuth or id-fpki-common-pivi-cardAuth ~~shall~~must only be used to authenticate the hardware token containing the associated private key and ~~shall~~must not be interpreted as authenticating the presenter or holder of the token.

Certificates intended for code signing are not permitted under this policy.

1.5. Policy Administration

1.5.1. Organization Administering the Document

The FPKIPA is responsible for all aspects of this CP.

1.5.2. Contact Person

~~Questions regarding this CP shall be directed to the Chair of the Federal PKI Policy Authority, whose address can be found at http://www.idmanagement.gov/fpkipa~~

Contact information for the support and co-chairs for the FPKIPA is fpki@gsa.gov.

1.5.3. Person Determining CPS Suitability for the Policy

The FPKIPA ~~shall~~must approve the CPS for each CA that issues certificates under this policy.

1.5.4. CPS Approval Procedures

CAs issuing under this ~~policy~~CP are required to meet all ~~facets of the policy.~~requirements. The FPKIPA will not issue waivers.

The FPKIPA ~~shall make~~makes the determination that a CPS complies with this policy. The CA and RA must ~~meet all requirements of~~operate under an approved CPS ~~before commencing operations.~~. RA practices are documented in the CPS or an associated Registration Practices

Statement (RPS). In ~~some cases, the FPKIPA may require the additional approval of an authorized agency. The FPKIPA will make this determination based on the nature of the system function, the type of communications, or the operating environment.~~

~~In~~ each case, the determination ~~of suitability shall be based on~~process must include an independent compliance auditor's results and recommendations. See Section 8 for further details.

1.6. Definitions and Acronyms

See ~~sections 11~~Appendix B and ~~12~~Appendix C.

2. Publication and Repository Responsibilities

2.1. Repositories

~~All CAs that issue certificates under this policy are obligated to post all CA certificates issued by or to the CA and CRLs issued by the CA in a repository that is publicly accessible through all Uniform Resource Identifier (URI) references asserted in valid certificates issued by that CA. Specific requirements are found in *Shared Service Provider Repository Service Requirements* [SSP REP]. CAs may optionally post subscriber certificates in this repository in accordance with agency policy, except as noted in section 9.4.3. To promote consistent access to certificates and CRLs, the repository shall implement access controls and communication mechanisms to prevent unauthorized modification or deletion of information.~~

~~Posted certificates and CRLs may be replicated in additional repositories for performance enhancement. Such repositories may be operated by the CA or other parties (e.g., Federal agencies).~~

~~2.2.1.1. Publication of Certification Information~~

~~2.2.1.1.1.1. Publication of Certificates and Certificate Status~~

The publicly accessible repository system ~~shall~~must be designed and implemented so as to provide 99% availability overall and limit scheduled down-time to 0.5% annually. ~~Where applicable, the certificate status server (CSS) shall be designed and implemented so as to provide 99% availability overall and limit scheduled down-time to 0.5% annually.~~

2.2. Publication of Certification Information

2.2.1. Publication of Certificates and Certificate Status

All CAs that issue CA certificates must publish all CA certificates it issues in a file available via a publicly accessible HTTP URI. This URI must be asserted in the Subject Information Access (SIA) extension in all valid certificates issued to the CA. The file must be a certs-only Cryptographic Message Syntax file that has an extension of .p7c.

With the exception of self-signed certificates, all CA certificates must be published by the Subject CA in a file available via a publicly accessible HTTP URI. This URI must be asserted in the Authority Information Access (AIA) extension in all valid certificates issued by the Subject CA. The file must be:

- a certs-only Cryptographic Message Syntax file that has an extension of .p7c, or
- a single DER encoded certificate that has an extension of .cer

The certs-only Cryptographic Message Syntax format is preferred as it allows flexibility for inclusion of multiple certificates.

All CAs that issue certificates under this policy must publish the latest CRL covering all unexpired certificates via a publicly accessible HTTP URI until such time as all issued certificates have expired. This URI must be asserted in the CRL distribution point extension of all certificates issued by that CA, with the exception of OCSP responder certificates that include the id-pkix-ocsp-nocheck extension.

A Certificate Status Server (CSS) provides status information about certificates on behalf of a CA through on-line transactions.

CAs must include a CSS in the form of a delegated Online Certificate Status Protocol (OCSP) service, as described in [RFC 6960], to provide on-line status information for Subscriber certificates via a publicly accessible HTTP URI in the AIA extension. The operations of the OCSP service are within the scope of this CP.

Pre-generated OCSP responses may be created by the CSS and distributed to OCSP servers. OCSP responses, like CRLs, are publicly distributable data. OCSP servers that lack OCSP response signing capability have the same security requirements as a repository hosting CRLs.

OCSP services that are locally trusted, as described in [RFC 6960], are not covered by this policy.

All certificates must contain only valid Uniform Resource Identifiers (URIs) that are publicly accessible by relying parties.

2.2.2. Publication of CA Information

~~The Common Policy~~This CP ~~shall~~must be publicly available on ~~the FPKIPA website (see http://www.idmanagement.gov/). A redacted version of~~ https://www.idmanagement.gov/.

The CPS and annual PKI Compliance Audit Letter for the Federal Common Policy ~~Root CAs will be~~CA are publicly available ~~from the FPKIMA website (See~~on ~~http://www.idmanagement.gov/).~~ https://www.idmanagement.gov/.

Other CAs operating under this policy ~~shall~~should make available a redacted CPS and annual PKI Compliance Audit Letter in their organization’s public repository.

~~2.2.3. Interoperability~~

~~Where certificates and CRLs are published in directories, standards-based schemas for directory objects and attributes shall be used as specified in the *Shared Service Provider Repository Service Requirements* [SSP-REP].~~

2.3. Time or Frequency of Publication

This CP and any subsequent changes ~~shall~~must be made publicly available within thirty (30) days of approval.

Publication requirements for CRLs are provided in Sections 4.9.7 and 4.9.12.

2.4. Access Controls on Repositories

~~The CA shall protect~~Repositories hosting CA certificates, CRLs, and pre-generated OCSP responses (if implemented) must be publicly accessible. Information not intended for modification or public dissemination ~~or modification. CA certificates and CRLs in the repository shall be publicly available through the Internet. Direct and/or remote access to other information in the CA repositories shall~~must be ~~determined by agencies pursuant to their authorizing and controlling statutes. The~~protected.

Each CPS ~~shall~~must detail what information in the repository ~~shall be~~is exempt from automatic availability and to whom, and under which conditions the restricted information may be made available.

Posted certificates, CRLs, and pre-generated OCSP responses may be replicated in additional repositories for performance enhancement.

3. Identification and Authentication

3.1. Naming

3.1.1. Types of Names

~~For certificates issued under id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-High, id-fpki-common-devices~~ This CP establishes requirements for both subject distinguished names and ~~id-fpki-common-devicesHardware~~ subject alternative names.

3.1.1.1. Subject Names

The CA ~~shall~~must assign X.501 distinguished names to all ~~subscribers.~~Subscriber certificates. These distinguished names are comprised of a base distinguished name (Base DN) and additional relative distinguished names (RDNs). Base DNs may be in either of two forms: a geo-political name or an Internet domain component name.

All geo-political distinguished names ~~assigned to federal employees shall be in~~must use one of the following ~~directory information tree~~Base DNs:

- C=US, o=U.S. Government, ~~[~~ou=department~~], [~~, ou=agency~~]~~, [ou=*structural_container*]
- C=US, o=U.S. Government, ou=department, [ou=*structural_container*]
- C=US, o=U.S. Government, ou=agency, [ou=*structural_container*]

The organizational units department and agency appear when applicable and are used to specify the federal entity that employs the ~~subscriber.~~Human Subscriber or owns the device. At least one of these organizational units must appear in the DN.

Distinguished names based on Internet domain component names must use the following Base DN:

- dc=gov, dc=org0, [dc=org1], …, [dc=orgN], [o=organization], [ou=*structural_container*]

At a minimum, the org0 domain component must appear in the Base DN. The org1 to orgN domain components appear, in order, when applicable, and are used to specify the federal entity that employs the Human Subscriber or owns the device.

The additional organizational unit *structural_container* in either the geo-political or Internet domain Base DN form is permitted to support local directory requirements, such as differentiation between Human Subscribers and ~~devices.~~Device Subscribers. This organizational unit may not be employed to further differentiate between subcomponents within an agency.

The distinguished name of the ~~federal employee subscriber shall take~~Human Subscriber must include a common name (CN) using one of the ~~three~~ following ~~forms~~formats:

- ~~C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*],~~Base DN, CN=nickname lastname
- ~~C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*],~~Base DN, CN=firstname initial. lastname
- ~~C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*],~~Base DN, CN=firstname initial lastname
- Base DN, CN=firstname middlename lastname
- Base DN, CN=lastname.firstname.middlename

In the first common name ~~form~~format, nickname may be the Human Subscriber's first name, a form of the first name, middle name, or pseudonym (e.g., Buck) by which the Subscriber is generally known. A generational qualifier, such as "Sr." or "III", or agency specific identifiers (e.g., CN=Giants.John.Gregory.1234567890) may be appended to any of the common name ~~forms~~formats specified above.

Additional certificate qualifiers may be appended to the common name in order to provide additional context to the certificate's intended usage. The qualifier must be preceded by a space followed by a hyphen (e.g., CN=John G. Giants -ENC).

Distinguished names assigned to federal contractors and other affiliated persons ~~shall be within the same directory information tree. The distinguished name of the federal contractor subscribers and affiliate subscribers will take~~must follow one of the ~~three following~~ name forms~~:~~

- ~~C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], cn=*nickname lastname* (affiliate)~~
- ~~C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], cn=*firstname initial. lastname* (affiliate)~~

- ~~C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], cn=*firstname middlename lastname* (affiliate)~~

~~For names assigned to federal contractors and other affiliated persons, generational qualifiers may be inserted between *lastname* and "(affiliate)".~~

~~Common name fields shall be populated as specified~~ identified above~~.~~ with (affiliate) appended to the end of the common name (e.g., CN=John G. Giants (affiliate)).

~~Distinguished names based on Internet domain component names shall be in the following directory information trees:~~

- ~~dc=gov, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*]~~
- ~~dc=mil, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*]~~

~~The default Internet domain name for the agency, [*orgN*.]…[*org0*].gov or [*orgN*.]…[*org0*].mil, will be used to determine DNs. The first domain component of the DN will either be dc=gov or dc=mil. At a minimum, the *org0* domain component must appear in the DN. The *org1* to *orgN* domain components appear, in order, when applicable and are used to specify the federal entity that employs the subscriber.~~

~~The distinguished name of the federal employee subscriber shall take one of the three following forms when their agency's Internet domain name ends in .gov:~~

- ~~dc=gov, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], cn=*nickname lastname*~~
- ~~dc=gov, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], cn=*firstname initial. lastname*~~
- ~~dc=gov, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], cn=*firstname middlename lastname*~~

~~The distinguished name of the federal contractors and affiliated subscribers shall take one of the three following forms when the agency's Internet domain name ends in .gov:~~

- ~~dc=gov, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], cn=*nickname lastname* (affiliate)~~
- ~~dc=gov, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], cn=*firstname initial. lastname* (affiliate)~~
- ~~dc=gov, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], cn=*firstname middlename lastname* (affiliate)~~

~~The distinguished name of the federal employee subscriber shall take one of the three following forms when their agency's Internet domain name ends in .mil:~~

- ~~dc=mil, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], cn=*nickname lastname*~~
- ~~dc=mil, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], cn=*firstname initial. lastname*~~
- ~~dc=mil, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], cn=*firstname middlename lastname*~~

~~The distinguished name of the federal contractors and affiliated subscribers shall take one of the three following forms when the agency's Internet domain name ends in .mil:~~

- ~~dc=mil, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], cn=*nickname lastname* (affiliate)~~

- ~~dc=mil, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], cn=*firstname initial. lastname* (affiliate)~~
- ~~dc=mil, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], cn=*firstname middlename lastname* (affiliate)~~

The CA may supplement any of the distinguished name forms for ~~users~~Human Subscribers specified in this section by including a dnQualifier, serial number, or user id~~ attribute~~. When any of these ~~attributes ~~are included, they may appear:

- as part of a multi-valued ~~relative distinguished name (~~RDN~~)~~ with the common name, or
- as a distinct RDN that follows the RDN containing the common name ~~attribute. Generational qualifiers may optionally be included in common name attributes in distinguished names based on Internet domain names. For names assigned to employees, generational qualifiers may be appended to the common name. For names assigned to federal contractors and other affiliated persons, generational qualifiers may be inserted between *lastname* and "(affiliate)".~~

Role-based signature certificates may be issued under id-fpki-common-hardware or id-fpki-common-high ~~may be issued with a ~~(see Section 1.3.4). For these certificates, the common name ~~that ~~specifies ~~an organizational ~~the role, ~~such as the head of an agency, ~~as follows:

- ~~C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], ~~CN=role [, department/agency]

- ~~dc=gov, dc=…, [ou=*structural_container*], cn=*role* [, *department/agency*]~~

~~The combination of organizational role and agency must unambiguously identify a single person. (That is, widely held roles such as *Computer Scientist* or *Procurement Specialist* cannot be included since they do not identify a particular person. *Chief Information Officer*, *AgencyX* could be included as it specifies a role held by a single person.)~~

Where the [department/agency] is implicit in the role (e.g., Secretary of Commerce), it should be omitted. Where the role alone is ambiguous (e.g., Chief Information Officer) the department/agency must be present in the common name. The organizational information in the common name must match that in the organizational unit attributes.

~~Practice Note: In the case of "Chief Information Officer", use of department/agency in the common name is redundant but is included for usability purposes. Display of the common name is widely supported in applications. Other attributes may or may not be presented to users.~~

~~Devices that are the~~

Practice Note: In the case of "Chief Information Officer", use of department/agency in the common name is redundant but is included for usability purposes. Display of the common name is widely supported in applications. Other attributes may or may not be presented to users.

Device Subscriber distinguished names must take the following form:

- Base DN, CN=device name

where device name is a descriptive name for the device.

When id-fpki-common-piv-contentSigning or id-fpki-common-pivi-contentSigning is asserted, the certificate's subject ~~of~~distinguished name must indicate the organization administering the credential issuance system.

When id-fpki-common-cardAuth is asserted, the certificate's subject distinguished name must take one of the following forms:

- Base DN, serialNumber=FASC-N
- Base DN, serialNumber=UUID

When id-fpki-common-pivi-cardAuth is asserted, the certificate's subject distinguished name must take the following form:

- Base DN, serialNumber=UUID

This CP does not restrict the subject distinguished names of CA certificates ~~issued under this policy shall be assigned~~and Delegated OCSP Responder certificates. However, CA certificates and Delegated OCSP Responder certificates must have subject distinguished names. CA and Delegated OCSP Responder certificate distinguished names may be either a geo~~-~~-political name or an Internet domain component name. Geo-political distinguished names must be composed of any combination of the following attributes: country; organization; organizational unit; and common name. Internet domain component names are composed of the following attributes: domain component; organizational unit; and common name. ~~Device names shall take one of the following forms:~~

- ~~C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=*structural_container*], cn=*device name*~~
- ~~dc=gov, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], [cn=*device name*]~~
- ~~dc=mil, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], [cn=*device name*]~~

~~where device name is a descriptive name for the device. Where~~CA subject distinguished names may or may not include a ~~device is fully described by the Internet domain name~~common name, for example:

Base DN, OU=Certification Authorities, OU=Agency CA

If included, the common name ~~attribute is optional~~in the CA certificates should describe the issuer, such as:

Base DN, OU=Certification Authorities, CN=AgencyX CA-3

3.1.1.2. Subject Alternative Names

Certificates issued under id-fpki-common-authentication or id-fpki-common-cardAuth must include a subject alternative name extension. The subject alternative name extension must include both:

- the pivFASC-N name type [FIPS 201], the value of which must be the FASC-N [PACS] of the subject's PIV credential; and
- a UUID encoded as a URI as specified in Section 3 of [RFC 4122].

Certificates issued under id-fpki-common-cardAuth must not include any other name in the subject alternative name extension.

Certificates issued under id-fpki-common-pivi-authentication, id-fpki-common-pivi-cardAuth, id-fpki-common-derived-pivAuth-hardware and id-fpki-common-derived-pivAuth must include a subject alternative name extension that includes:

- a UUID encoded as a URI as specified in Section 3 of [RFC 4122].
- for derived PIV, UUID is unique per certificate

Certificates issued under id-fpki-common-pivi-cardAuth must not include any other name in the subject alternative name extension.

Subscriber certificates that contain id-kp-emailProtection in the EKU must include a subject alternative name extension that includes a rfc822Name.

For Device Subscriber certificates that assert serverAuth in the ~~EKU~~Extended Key Usage:

- A subject alternative name of type dNSName must be included.
- Wildcard domain names are permitted in the dNSName values only if all sub-domains covered by the wildcard fall within the same application, cloud service, or system accreditation boundary within the scope of the sponsoring agency.
- Wildcards ~~shall~~must not be used in subdomains that host more than one distinct application platform. The use of third-level agency wildcards, (e.g., *.[agency].gov), ~~shall~~must be prohibited to reduce the likelihood that a certificate will overlap multiple systems or services. Third level wildcards are permitted for ~~DNS names~~dNSName dedicated to a specific application (e.g., *.[application_name].gov).
- Before ~~issuing~~requesting a serverAuth certificate containing a wildcard, the ~~CA shall ensure the~~ sponsoring agency ~~has a documented procedure for determining~~must provide evidence to the issuing CA that the scope of the certificate does not now and will not infringe on other agency applications.

~~This policy does not restrict the directory information tree for names of CAs and CSSs. However, CAs that issue certificates under this policy must have distinguished names. CA and CSS distinguished names may be either a geo-political name or an Internet domain component name.~~

~~CA and CSS geo-political distinguished names shall be composed of any combination of the following attributes: country; organization; organizational unit; and common name.~~

~~Internet domain component names are composed of the following attributes: domain component; organizational unit; and common name.~~

~~The Common PIV Content Signing certificate's subject DN shall indicate the organization administering the PIV card issuance system or device according to types of names for devices.~~

~~Certificates issued under id-fpki-common-derived-pivAuth-hardware and id-fpki-common-derived-pivAuth shall include a non-empty subject DN and shall also include a subject alternative name extension that includes a UUID, which shall be encoded as a URI as specified in Section 3 of [RFC 4122]. A unique UUID shall be created for each certificate issued under one of these policies. For certificates issued under this policy by a CA operating as part of the Shared Service Providers program, subject distinguished names shall follow either the rules specified above for id-fpki-common-hardware or the rules specified below for including a non-NULL subject DN with a UUID in id-fpki-common-cardAuth. For legacy Federal PKIs only, distinguished names may follow established agency naming conventions.~~

~~For certificates issued under id-fpki-common-authentication or id-fpki-common-pivi-authentication, assignment of X.500 distinguished names is mandatory. For certificates issued under this policy by a CA operating as part of the Shared Service Providers program, distinguished names shall follow either the rules specified above for id-fpki-common-hardware or the rules specified below for including a non-NULL subject DN in id-fpki-common-cardAuth. For legacy Federal PKIs only, distinguished names may follow established agency naming conventions. Certificates issued under id-fpki-common-authentication or id-fpki-common-pivi-authentication shall include a subject alternative name.~~

~~For certificates asserting id-fpki-common-authentication, at a minimum, the subject alternative name extension shall include:~~

1) ~~the pivFASC-N name type [FIPS 201]. The value for this name shall be the FASC-N [PACS] of the subject's PIV card~~
2) ~~The UUID [RFC 4122]~~

~~For certificates asserting id-fpki-common-pivi-authentication, at a minimum, the subject alternative name extension shall include:~~

1) ~~The UUID [RFC 4122]~~

~~Certificates issued under id-fpki-common-cardAuth shall include a subject alternative name extension that includes the pivFASC-N name type. The value for this name shall be the FASC-N of the subject's PIV card. Certificates issued under id-fpki-common-cardAuth shall also include a UUID [RFC 4122] in the subject alternative name extension, as specified in Section 3.3 of [SP 800-73-3(1)]. Certificates issued under id-fpki-common-pivi-cardAuth shall only include a UUID [RFC 4122] in the subject alternative name extension. Certificates issued under id-fpki-common-cardAuth or id-fpki-common-pivi-cardAuth shall not include any other name in the subject alternative name extension but may include a non-NULL name in the subject field. If~~

~~included, the subject distinguished name shall take one of the following forms:~~

~~PIV Examples:~~

- ~~C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], serialNumber=*FASC-N*~~
- ~~dc=gov, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], serialNumber=*FASC-N*~~
- ~~dc=mil, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], serialNumber=*FASC-N*~~

~~PIV or PIV-I Examples:~~

- ~~C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], serialNumber=*UUID*~~
- ~~dc=gov, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], serialNumber=*UUID*~~
- ~~dc=mil, dc=*org0*, [dc=*org1*], …, [dc=*orgN*], [ou=*structural_container*], serialNumber=*UUID*~~

~~Practice Note: The FASC-N [PACS] consists of 40 decimal digits that are encoded as a 25-byte binary value. This 25-byte binary value may be encoded directly into the pivFASC-N name type in the subject alternative name extension, but when included in the subject field the FASC-N must be encoded as a PrintableString that is at most 64 characters long. This policy does not mandate any particular method for encoding the FASC-N within the serial number attribute as long as the same encoding method is used for all certificates issued by a CA. Acceptable methods for encoding the FASC-N within the serial number attribute include encoding the 25-byte binary value as 50 bytes of ASCII HEX or encoding the 40 decimal digits as 40 bytes of ASCII decimal.~~

~~Practice Note: When the UUID appears in the subjectAltName extension of a certificate, it must be encoded as a uniformResourceIdentifier as specified in Section 3 of [RFC 4122]. An example of a UUID encoded as a URI, from RFC 4122, is "urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6". This policy does not mandate any particular method for encoding the UUID within the serial number attribute as long as the same encoding method is used for all certificates issued by the CA and it is encoded as a PrintableString that is at most 64 characters long, however, it is recommended that the string representation from Section 3 of [RFC 4122] be used. An example would be "f81d4fae-7dec-11d0-a765-00a0c91e6bf6".~~

Section 3.1 Practice Note: The FASC-N [PACS] consists of 40 decimal digits that are encoded as a 25-byte binary value. This 25-byte binary value may be encoded directly into the pivFASC-N name type in the subject alternative name extension, but when included in the subject distinguished name the FASC-N must be encoded as a PrintableString that is at most 64 characters long. This policy does not mandate any particular method for encoding the FASC-N within the serial number attribute as long as the same encoding method is used for all certificates issued by a CA. Acceptable methods for encoding the FASC-N within the serial number attribute include encoding the 25-byte binary value as 50 bytes of ASCII HEX or encoding the 40 decimal digits as 40 bytes of ASCII decimal.

Section 3.1 Practice Note: When the UUID appears in the subject alternative name extension of a certificate, it must be encoded as a uniformResourceIdentifier as specified in Section 3 of [RFC 4122]. An example of a UUID encoded as a URI, from RFC 4122, is “urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6”. This policy does not mandate any particular method for encoding the UUID within the serial number attribute as long as the same encoding method is used for all certificates issued by the CA and it is encoded as a PrintableString that is at most 64 characters long. However, it is recommended that the string representation from Section 3 of [RFC 4122] be used. An example would be “f81d4fae-7dec-11d0-a765-00a0c91e6bf6”.

3.1.2. Need for Names to Be Meaningful

~~The~~ Subscriber certificates ~~issued pursuant to this CP~~ are meaningful only if the names that appear in the certificates can be understood and used by relying parties. Names used in the certificates must identify in a meaningful way the Subscriber to which they are assigned.

The common name in the ~~DN~~distinguished name must represent the Subscriber in a way that is easily understandable for humans. For ~~people~~Human Subscribers, this will typically be a legal name, ~~so the preferred common name form is~~

~~cn=*firstname initial. lastname*~~

~~While the issuer name in CA certificates is not generally interpreted by relying parties, this CP still requires use of meaningful names by CAs issuing under this policy. If included, the common name should describe the issuer, such as:~~

~~cn=*AgencyX CA*~~ see Section 3.1.1.

The subject name in CA certificates must match the issuer name in certificates issued by the subject, as required by [RFC 5280~~.~~].

3.1.3. Anonymity or Pseudonymity of Subscribers

~~The~~A CA ~~shall~~must not issue anonymous certificates. ~~Pseudonymous~~

Role-based certificates may be issued by the CA to support internal operations. CAs may also issue ~~pseudonymous~~role-based certificates that identify subjects by their organizational roles, as described in Section 3.1.1.

CA certificates ~~issued by the CA shall~~must not contain anonymous or pseudonymous identities.

3.1.4. Rules for Interpreting Various Name Forms

Rules for interpreting distinguished name forms are specified in [X.501~~.~~]. Rules for interpreting e~~-~~-mail addresses are specified in [RFC 5322]. Rules for interpreting the pivFASC-N name type are specified in [PACS].

3.1.5. Uniqueness of Names

Name uniqueness for certificates issued by each CA must be enforced. Each CA and its associated RAs ~~shall~~must enforce name uniqueness within the X.500 ~~name space.~~namespace. When other name forms are used, they too must be allocated such that name uniqueness is ensured for certificates issued by that CA. Name uniqueness is not violated when multiple certificates are issued to the same entity.

~~Practice Note: For distinguished names, name uniqueness is enforced for the entire name rather than a particular attribute (e.g., the common name).~~

Practice Note: For distinguished names, name uniqueness is enforced for the entire name rather than a particular attribute (e.g., the common name).

The CPS ~~shall~~must identify the method for the assignment of subject names. ~~Directory information trees may be assigned to a single CA, or shared between CAs. Where multiple CAs share a single directory information tree, the FPKIPA shall review and approve the method for assignment of subject names.~~

3.1.6. Recognition, Authentication, and Role of Trademarks

CAs operating under this policy ~~shall~~must not issue a certificate knowing that it infringes the trademark of another. The FPKIPA ~~shall~~must resolve disputes involving names and trademarks.

3.2. *Initial Identity Validation*

3.2.1. Method to Prove Possession of Private Key

~~In all cases where~~The CA must verify the ~~party named in a certificate generates its own keys, that party shall be required to prove~~Applicant has possession of the private key~~, which~~ that corresponds to the public key in the certificate request. As an example, for signature keys~~,~~ this may be done by the ~~entity~~Applicant using its private key to sign a value supplied by the CA. The CA ~~shall~~must then validate the signature using the ~~party's~~Applicant's public key. The FPKIPA may allow other mechanisms that are at least as secure as those cited here.

In the case where key generation is performed under the CA or RA's direct control, proof of possession is not required. (e.g., key management certificates generated in a system allowing key escrow.)

3.2.2. Authentication of Organization Identity

Requests for CA certificates ~~shall~~must include the CA name, address, and documentation of the existence of the CA. Before issuing CA certificates, an authority for the issuing CA ~~shall~~must verify the information provided by the requesting organization, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the ~~CA~~organization.

Before issuing subscriber certificates on behalf of an organization, the issuing CA must verify the authority of requesting representatives.

3.2.3. Authentication of Individual Identity

~~This policy allows a certificate to be issued only to a single entity. Certificates shall not be issued that contain a public key whose associated private key is shared.~~

For each certificate issued, the CA must authenticate the identity of the individual requester.

3.2.3.1. Authentication of Human Subscribers

Procedures used by agencies to ~~issue identification to~~authenticate the identity of their own personnel and affiliates may be more stringent than that set forth below. When this is the case, the agency procedures for authentication of the identity of personnel ~~shall~~must apply in addition to the ~~guidance~~requirements in this section.

The RA ~~shall~~must ensure that the Applicant's identity information is verified. ~~Identity shall be verified no more than 30 days before initial certificate issuance.~~

~~At id-fpki-common-High, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-authentication, and id-fpki-common-pivi-authentication, the applicant shall appear at the RA in person or via supervised remote[1]. For all other policies, RAs may accept authentication of an applicant's identity attested to and documented by a trusted agent, assuming agency identity badging requirements are otherwise satisfied. Authentication by a trusted agent does not relieve the RA of its responsibility to verify required procedures were followed as described below.~~

At a minimum, ~~authentication~~ procedures for employees must include the following steps:

1. Verify that a request for certificate issuance to the Applicant was submitted by agency management.
2. Verify Applicant's employment through use of official agency records.
3. Establish Applicant's identity by in-person or supervised remote[2] proofing before the ~~registration authority~~RA or trusted agent, as follows:

~~[1] The minimum requirements associated with supervised remote identity proofing are described in NIST SP 800-63A, *Digital Identity Guidelines: Enrollment and Identity Proofing*, Section 5.3.3. In addition, the supervised remote process must have the capability of capturing an approved biometric.~~

[2] The minimum requirements associated with supervised remote identity proofing are described in NIST SP 800-63A, *Digital Identity Guidelines: Enrollment and Identity Proofing*, Section 5.3.3. In addition, the supervised remote process must have the capability of capturing an approved biometric.

    a. The Applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver’s license) as proof of identity, and
    b. The RA examines the presented credential for biometric data that can be linked to the Applicant (e.g., a photograph on the credential itself or a securely linked photograph of Applicant), and
    c. The credential presented in step ~~3) a)~~3a above ~~shall~~must be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). Typically, this is accomplished by querying a database maintained by the organization that issued the credential, but other equivalent methods may be used.

4. Record and maintain a biometric of the Applicant (e.g., a photograph or fingerprint) by the RA or CA. (Handwritten signatures and other behavioral characteristics are not accepted as biometrics for the purposes of this policy.) This establishes an audit trail for dispute resolution.

For contractors and other affiliated personnel, the~~ authentication~~ procedures must include the following steps:

1. Verify that a request for certificate issuance to the Applicant was submitted by an authorized sponsoring agency employee (e.g., contracting officer or contracting officer’s technical representative).
2. Verify sponsoring agency employee’s identity and employment as follows:
    a. A digitally signed request from the sponsoring agency employee, verified by a currently valid employee signature certificate issued by an agency CA, may be accepted as proof of both employment and identity,
    b. Authentication of the sponsoring agency employee with a valid employee PIV-authentication certificate issued by the agency may be accepted as proof of both employment and identity, or
    c. In-person or supervised remote identity proofing of the sponsoring agency employee may be established before the registration authority as specified in employee authentication above and employment validated through use of the official agency records.
3. Establish Applicant’s identity by in-person or supervised remote proofing before the registration authority or trusted agent, as follows:
    a. The Applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver’s license) as proof of identity, and
    b. The RA examines the presented credential for biometric data that can be linked to the Applicant (e.g., a photograph on the credential itself or a securely linked photograph of Applicant), and
    c. The credential presented in step ~~3) a)~~3a above ~~shall~~must be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). Typically, this is accomplished by querying official records maintained by the organization that issued the credential.

4. Record and maintain a biometric of the Applicant (e.g., a photograph or fingerprint) by the RA or CA. (Handwritten signatures and other behavioral characteristics are not accepted as biometrics for the purposes of this policy.) This establishes an audit trail for dispute resolution.

In the event an Applicant is denied a credential based on the results of the identity proofing process, the ~~Entity shall~~sponsoring agency must provide a mechanism for appeal or redress of the decision.

Additionally, the RA ~~shall~~must record the process that was followed for issuance of each certificate. The process documentation and authentication requirements ~~shall~~must include the following:

- The identity of the person performing the ~~identification;~~authentication and either:
  - A signed declaration by that person that he or she verified the identity of the Applicant ~~as required by the CPS~~ using the format set forth at [28 U.S.C. 1746] (declaration under penalty of perjury); or
  - An auditable record identifying the person performing the identification and recording the assertion that he or she verified the identity of the Applicant.
- Unique identifying number(s) from the ID(s) of the Applicant, or a facsimile of the ID(s);
- The biometric of the Applicant;
- The date and time of the verification; and~~Unique identifying number(s) from the ID(s) of the Applicant, or a facsimile of the ID(s);~~
- ~~The biometric of the Applicant;~~
- ~~The date and time of the verification; and~~ either:
  - An auditable record indicating the applicant accepted the certificate; or
  - A declaration of identity signed by the Applicant using a handwritten signature or appropriate digital signature and performed in the presence of the person performing the identity authentication, using the format set forth at [28 U.S.C. 1746] (declaration under penalty of perjury).

For certificates issued under id-fpki-common-authentication, id-fpki-common-pivi-authentication, id-fpki-common-pivi-cardAuth, and id-fpki-common-cardAuth, identity must be verified in accordance with the requirements specified for issuing PIV in Section 2.7 of [FIPS 201].

At id-fpki-common-High, id-fpki-common-authentication, and id-fpki-common-pivi-authentication, the Applicant must appear at the RA in person or via supervised remote.

For id-fpki-common-policy and id-fpki-common-hardware, RAs may accept authentication of an Applicant's identity attested to and documented by a trusted agent, assuming agency identity requirements are otherwise satisfied. Authentication by a trusted agent does not relieve the RA of its responsibility to verify required procedures were followed as described above.

For certificates issued under id-fpki-common-derived-pivAuth-hardware and id-fpki-common-derived-pivAuth, identity must be verified in accordance with the requirements specified for issuing derived credentials in [SP 800-157]. At id-fpki-common-derived-pivAuth-hardware, the Applicant must appear at the RA in person or via supervised remote.

The RA or CA must:

1) Verify that the request for certificate issuance to the Applicant was submitted by an authorized agency employee.
2) Use the PKI-AUTH authentication mechanism from Section 6 of [FIPS 201] to verify that the PIV Authentication certificate on the Applicant's PIV credential is valid and that the Applicant is in possession of the corresponding private key.
3) Maintain a copy of the Applicant's PIV Authentication certificate.

Seven days after issuing the derived credential, the CA should recheck the revocation status of the PIV Authentication certificate. This step can detect use of a compromised PIV credential to obtain a derived credential.

For certificates issued under id-fpki-common-derived-pivAuth-hardware, the Applicant must appear in person or via supervised remote to present the PIV credential and perform the PKI-AUTH authentication mechanism. The RA must perform a one-to-one comparison of the Applicant against biometric data stored on the PIV credential, in accordance with [SP 800-76], and must record and maintain the biometric sample used to validate the Applicant.

In cases where a 1:1 biometric match against the biometrics available on the PIV credential or in the chain-of-trust, as defined in [FIPS 201] is not possible:

1) The Applicant must present a government-issued form of identification (e.g., a passport or driver's license) in addition to the PIV credential, and
2) The RA must examine the presented credentials for biometric data that can be linked to the Applicant (e.g., a photograph on the credential itself or a securely linked photograph of the Applicant), and

The process documentation and authentication requirements must include the following:

- The identity of the person performing the authentication and either:
  - A signed declaration by that person that he or she verified the identity of the Applicant using the format set forth at [28 U.S.C. 1746] (declaration under penalty of perjury); or
  - An auditable record linking the authentication of the person performing the identification to their verification of each Applicant.
- Unique identifying number(s) from second form of identification of the Applicant, or a facsimile of the ID(s);
- The biometric of the Applicant;
- The date and time of the verification;

3.2.3.2. Authentication of Devices

Some computing and communications devices (routers, firewalls, servers, etc.) and software applications will be named as certificate subjects. In such cases, the device must have a human sponsor who is affiliated with the agency under which the certificate is being issued. The sponsor is responsible for providing the following registration information:

- Equipment identification (e.g., serial number) or service name (e.g., DNS name) or unique software application name
- Equipment or software application public keys
- Equipment or software application authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the sponsor when required.

These certificates ~~shall~~must be issued only to authorized devices under the subscribing organization's control. In the case a human sponsor is changed, the new sponsor ~~shall~~must review the status of each device under his/her sponsorship to ensure it is still authorized to receive certificates. The CPS ~~shall~~must describe procedures to ensure that certificate accountability is maintained. See Section 9.6.3 for Subscriber responsibilities.

Before issuing a certificate with a wildcard character (*) in a ~~CN~~common name or ~~subjectAltName~~subject alternative name of type ~~DNS-ID~~dNSName, the CA ~~shall~~must establish and follow a documented procedure to ensure that the wildcard does not fall immediately to the left of an agency or organization name, but is qualified down to a unique application, server, or server farm under control of the sponsor's organization~~.~~ (see Section 3.1.1). The device sponsor ~~shall~~must demonstrate that the domain name requested is entirely within the ~~name space~~namespace to be covered by the wildcard certificate.

The identity of the sponsor ~~shall~~must be authenticated by:

- Verification of digitally signed messages sent from the sponsor using a certificate issued under this policy; or
- In-person or supervised remote registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of Section 3.2.3.1.

~~*3.2.3.3. Authentication for Derived PIV Credentials*~~

~~For certificates issued under id-fpki-common-derived-pivAuth-hardware and id-fpki-common-derived-pivAuth, identity shall be verified in accordance with the requirements specified for issuing derived credentials in [SP 800-157]. The RA or CA shall:~~

~~1) Verify that the request for certificate issuance to the Applicant was submitted by an authorized agency employee.~~

~~1) Use the PKI-AUTH authentication mechanism from Section 6 of FIPS 201 to verify that the PIV Authentication certificate on the applicant's PIV Card is valid and that the applicant is in possession of the corresponding private key.~~

~~2)1) Maintain a copy of the Applicant's PIV Authentication certificate.~~

~~Seven days after issuing the Derived credential, the issuer should recheck the revocation status of the PIV Authentication certificate. This step can detect use of a compromised PIV Card to obtain a derived credential~~

~~For certificates issued under id-fpki-common-derived-pivAuth-hardware, the applicant shall appear in person or via supervised remote to present the PIV Card and perform the PKI-AUTH authentication mechanism. The RA shall perform a one-to-one comparison of the applicant against biometric data stored on the PIV Card, in accordance with [SP 800-76], and shall record and maintain the biometric sample used to validate the applicant. In cases where a 1:1 biometric match against the biometrics available on the PIV Card or in the chain-of-trust, as defined in [FIPS201] is not possible:~~

~~1) The applicant shall present a government-issued form of identification (e.g., a passport or driver's license) in addition to the PIV Card, and~~

~~1) The RA shall examine the presented credentials for biometric data that can be linked to the Applicant (e.g., a photograph on the credential itself or a securely linked photograph of the Applicant), and~~

~~2) The process documentation for the issuance of the certificate shall include the identity of the person performing the verification of the second (non-PIV) form of identification, a signed declaration by that person that he or she verified the identity of the applicant as required by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury), a unique identifying number from the second form of identification or a facsimile of the ID, a biometric of the applicant, and the date and time of the verification.~~

3.2.4. Non-verified Subscriber Information

~~Information that is not verified shall not be~~ All Subscriber information included in certificates must be verified.

3.2.5. Validation of Authority

~~Before issuing~~ The CA ~~certificates or signature certificates that assert organizational authority, the CA shall~~must validate the ~~individual's~~requestor's authority to act in the name of the organization~~. For pseudonymous~~ before issuing organizational certificates, such as CA certificates, role-based certificates ~~that identify subjects by their organizational roles~~, or content signing certificates.

For example, before issuing role-based certificates, the CA ~~shall~~must validate that the individual either holds that role or has been delegated the authority to sign on behalf of the role.

In accordance with Section 3.2.3.2, all requests for device certificates in the name of an organization, ~~shall~~must be digitally signed by the sponsor. In addition, the CPS ~~shall~~must specify a process by which an organization identifies the individuals who may request certificates that assert organizational authority. If an organization specifies, in writing, the individuals who may request a certificate, then the CA ~~shall~~must not accept any certificate requests that are outside this specification. The CA ~~shall~~must provide an Applicant with a list of the organization’s authorized certificate ~~requesters~~requestors upon the Applicant’s verified written request.

~~Practice Note: Examples of signature certificates that assert organizational authority are code signing certificates and FIPS 201 id-PIV-content-signing certificates.~~

3.2.6. Criteria for Interoperation

The FPKIPA ~~shall~~must determine the interoperability criteria for CAs operating under this policy.

3.3. Identification and Authentication for Re-Key Requests

3.3.1. Identification and Authentication for Routine Re-key

CA certificate re-key ~~shall~~must follow the same procedures as initial certificate issuance.

PIV subscriber's identity should be established through the use of a current signature key, except that identity must be re-established and biometrics re-collected through an in-person or supervised remote registration at least every twelve years.

In the event a PIV Subscriber's signature key cannot be used, identity may be verified through the use of biometrics on file through the chain of trust defined in [FIPS 201].

For re-key of Human Subscriber certificates issued under id-fpki-common-high, identity may be established through use of current signature key, except that identity must be established through an in-person registration process at least once every three years from the time of initial registration.

For id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-authentication, id-fpki-common-pivi-authentication, id-fpki-common-derived-pivAuth, and id-fpki-common-derived-pivAuth-hardware, a Human Subscriber’s identity may be established through use of current signature key, except that identity must be re-established through an in-person or supervised remote registration process at least once every twelve years from the time of initial registration.

For re-key of Subscriber certificates issued under id-fpki-common-derived-pivAuth and id-fpki-common-derived-pivAuth-hardware, the department or agency ~~shall~~must verify that the Subscriber is eligible to have a PIV ~~Card~~credential (i.e., PIV ~~Card~~credential is not terminated).

~~For re-key of subscriber certificates issued under id-fpki-common-High, identity may be established through use of current signature key, except that identity shall be established through an in-person registration process at least once every three years from the time of initial registration.~~

~~For policies other than id-fpki-common-High, a subscriber’s identity may be established through use of current signature key, except that identity shall be re-established through an in-person or~~

~~supervised remote registration process at least once every nine years from the time of initial registration.~~

~~In addition,~~ For re-key of Subscriber certificates issued under id-fpki-common-derived-pivAuth-hardware, identity ~~shall~~must be established via mutual authentication between the issuer and the cryptographic module containing the current key, if the new key will be stored in the same cryptographic module as the current key. Identity ~~shall~~must be established through the initial registration process per Section 3.2 if the new key will be stored in a different cryptographic module than the current key.

For Device ~~certificates~~Subscribers, identity may be established through the use of the device's current signature key or the signature key of the device's human sponsor~~, except that identity shall be established through the initial registration process at least once every nine years from the time of initial registration~~.

3.3.2. Identification and Authentication for Re-key after Revocation

In the event of certificate revocation, issuance of a new certificate ~~shall always~~must require that the ~~party~~Applicant go through the initial registration process per Section 3.2 above~~.~~, unless identity can be verified through the use of biometrics on file through the chain of trust defined in [FIPS 201].

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Revocation requests must be authenticated. Note that revocation requests may be digitally signed using a certificate's private key, regardless of whether or not the private key has been compromised.
~~Requests to revoke a certificate may be authenticated using that certificate's public key, regardless of whether or not the associated private key has been compromised.~~

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. CERTIFICATE APPLICATION

The Certificate application process must provide sufficient information to:

- Establish the Applicant's authorization ~~(~~by the employing or sponsoring agency~~)~~ to obtain a certificate. ~~(per~~ See Section 3.2.3~~)~~ for requirements.
- Establish and record the identity of the Applicant. ~~(per~~ See Section 3.2.3~~)~~ for requirements.
- Obtain the Applicant's public key and verify the Applicant's possession of the private key ~~for each certificate required. (per~~. See Section 3.2.~~1)~~3 for requirements.
- Verify ~~any role or authorization~~ the information ~~requested for inclusion~~included in the certificate.

These steps may be performed in any order ~~that is convenient for the PKI Authorities and applicants that does not defeat security~~, but all must be completed before certificate issuance.

4.1.1. Who Can Submit a Certificate Application

~~4.1.1.1. CA Certificates~~

~~An application for a CA certificate shall be submitted by an authorized representative of the applicant CA.~~

~~4.1.1.2. User Certificates~~

~~An application for a user (subscriber) certificate shall be submitted by either the applicant or a trusted agent.~~

~~4.1.1.3. Device Certificates~~

~~An application for a device certificate shall be submitted by the human sponsor of the device.~~

~~4.1.1.4. Code Signing Certificates~~

~~A code signing certificate has an Extended Key Usage (EKU) containing a value of id-kp-codeSigning OBJECT IDENTIFIER ::= { id-kp 3 }(1.3.6.1.5.5.7.3.3).~~

~~An application for a code signing certificate shall be submitted by an authorized representative of the organization.~~

Type of Certificate	Who can submit an application?
CA and Delegated OCSP Responder Certificates	Authorized representative of the CA
Human Subscriber Certificate	An authorized agency official, the Applicant, or a Trusted Agent on behalf of the Applicant
Device Certificate	The human sponsor of the device

4.1.2. Enrollment Process and Responsibilities

All communications ~~among PKI Authorities~~ supporting the certificate application and issuance process ~~shall~~must be authenticated and protected from modification~~; any electronic transmission of shared secrets shall be protected. ~~. Communications may be electronic or out-of-band.

Any electronic communication of shared secrets must be protected.

Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair ~~shall~~must be used.

Out-of-band communications ~~shall~~must protect the confidentiality and integrity of the data.

Subscribers are responsible for providing accurate information on their certificate applications.

4.2. *CERTIFICATE APPLICATION PROCESSING*

Information in certificate applications must be verified as accurate before certificates are issued. ~~PKI Authorities shall~~Each CPS must specify procedures to verify information in certificate applications.

4.2.1. Performing Identification and Authentication Functions

The identification and authentication of the Subscriber must meet the requirements specified for Subscriber authentication as specified in Sections 3.2 and 3.3 of this CP.~~ The PKI Authority must identify the components of the PKI Authority (e.g., CA or RA) that are responsible for authenticating the subscriber's identity in each case.~~

4.2.2. Approval or Rejection of Certificate Applications

~~For the Common Policy Root CAs, ~~The FPKIPA may approve or reject ~~a~~requests for certificates from the Federal Common Policy CA.

Subscriber certificate ~~application.~~

~~For CAs operating under this policy, ~~approval or rejection ~~of certificate applications ~~is at the discretion of the Agency~~ PMA or its designee~~.

~~For Device certificates, the CA shall~~CAs must reject a certificate request if the requested public key has a known weak private key.

Public key parameters generation and quality checking~~, shall~~ must be conducted in accordance with [NIST SP 800-89~~.~~]. Key validity ~~shall~~must be confirmed in accordance with [NIST SP 800-56A~~.~~].

4.2.3. Time to Process Certificate Applications

Certificate applications must be processed and a certificate issued within ~~30~~90 days of identity verification.

4.3. *CERTIFICATE ISSUANCE*

4.3.1. CA Actions During Certificate Issuance

Upon receiving the request, the CAs/RAs will~~—~~:

- Verify the identity of the ~~requester~~requestor.
- Verify the authority of the ~~requester~~requestor and the integrity of the information in the certificate request.
- Build and sign a certificate if all certificate requirements have been met (in the case of an RA, have the CA sign the certificate).
- Make the certificate available to the Subscriber after confirming that the Subscriber has formally acknowledged ~~their~~the obligations~~ as~~ described in Section 9.6.3.

The certificate request may already contain a certificate built by either the RA or the Subscriber. This certificate will not be signed until all verifications and modifications, if any, have been completed to the CA's satisfaction.

~~All authorization and other~~All attribute information received from a prospective Subscriber ~~shall~~must be verified before inclusion in a certificate.~~ The responsibility for verifying prospective subscriber data shall be described in a CA's CPS.~~

4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

CAs operating under this policy ~~shall~~must inform the Subscriber (or other certificate subject) of the creation of a certificate and make the certificate available to the Subscriber. For device certificates, the CA ~~shall~~must inform the human sponsor.

4.4. CERTIFICATE ACCEPTANCE

Before ~~a subscriber~~Human Subscribers can ~~make effective~~ use ~~of its~~their private ~~key, a PKI Authority shall explain to~~keys, they must accept the ~~subscriber its~~ responsibilities ~~as~~ defined in Section 9.6.3 by accepting the Subscriber agreement.

4.4.1. Conduct Constituting Certificate Acceptance

For CA certificates issued by the Federal Common Policy ~~Root~~ CA, failure to object to the certificate or its contents ~~shall constitute~~constitutes acceptance of the CA certificate.

~~For all other CAs operating under this policy, no stipulation.~~

For certificates issued to Subscribers, a signed Subscriber agreement or auditable record of acceptance constitutes acceptance of the certificates.

4.4.2. Publication of the Certificate by the CA

As specified in Section 2.1, all CA certificates ~~shall~~must be published in repositories.

Certificates that contain the FASC-N and/or UUID in the subject alternative name extension, such as PIV Authentication Certificates, must not be distributed via public repositories (e.g., via LDAP or HTTP). This policy makes no other stipulation regarding publication of Subscriber certificates~~, except as noted in section 9.4.3.~~.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

~~4.4.3. Notification of Certificate Issuance by the CA to Other Entities~~

~~Whenever a CA operating under this policy issues a CA certificate,~~ The FPKIPA ~~shall~~must be notified at least two weeks prior to issuance~~.~~ of a CA certificate. In addition, ~~all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the event shall~~notification must be provided to the FPKIPA ~~within 24 hours following issuance~~when the CA certificate is published.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber Private Key and Certificate Usage

The intended scope of usage for a private key is specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate.

4.5.2. Relying Party Public key and Certificate Usage

Common Policy-issued certificates specify restrictions on use through ~~critical ~~certificate extensions, including the basic constraints and key usage extensions. ~~All CAs operating under this policy shall issue CRLs specifying the current~~CAs provide certificate status ~~of all unexpired certificates (except for OCSP responder certificates that include the id-pkix-ocsp-nocheck extension). It is recommended that~~information. Relying parties should process certificate and ~~comply with this~~status information ~~whenever using~~as specified in [X.509] when relying on Common Policy certificates~~ in a transaction~~.

4.6. CERTIFICATE RENEWAL

Renewing a certificate means creating a new certificate with ~~the same name, key, and other~~a new serial number where all certificate subject information~~ as the old one, but with a new,~~, including the subject public key and subject key identifier, remain unchanged.

The new certificate may have an extended validity period and ~~a new serial number. ~~may include new issuer information (e.g. different CRL distribution point, AIA and/or be signed with a different issuer key).

Once renewed, the old certificate may or may not be revoked~~,~~ but must not be reused for requesting further renewals, re-~~keyed, renewed~~keys, or ~~modified~~modifications.

4.6.1. Circumstance for Certificate Renewal

Subscriber certificates issued under this policy ~~shall~~must not be renewed, except during recovery from CA key compromise (see Section 5.7.3). In such cases, the renewed certificate ~~shall~~must expire as specified in the original Subscriber certificate.

CA certificates and Delegated OCSP responder certificates may be renewed so long as the aggregated lifetime of the ~~public~~private key does not exceed the ~~certificate lifetime~~requirements specified in Section 6.3.2.

~~The CA may automatically renew certificates during recovery from key compromise.~~

4.6.2. Who May Request Renewal

For ~~all CAs~~the Federal Common Policy CA, the FPKIMA may request renewal of CA certificates it issues.

For other CA certificates and Delegated OCSP ~~responders operating under this policy~~responder certificates, the corresponding operating authority may request renewal~~ of its own certificate. For the Common Policy Root CA, the FPKIMA may also request renewal of CA certificates~~.

4.6.3. Processing Certificate Renewal Requests

~~For~~When a CA re-keys, it may renew the ~~Common Policy Root CA, ~~certificates it has issued.

When certificates are renewed as a result of CA key compromise, as described in Section 4.6.1, the CA or RA must verify all certificates issued since the date of compromise were issued appropriately. If the certificate ~~renewal for reasons other than re-key of the Common Policy Root CA shall~~cannot be ~~approved by the FPKIPA~~verified, then it must not be renewed.

~~For all other renewal requests, no stipulation.~~

4.6.4. Notification of New Certificate Issuance to Subscriber

~~The CA shall inform the subscriber of the renewal of his or her certificate and the contents of the certificate.~~

As specified in Section 4.3.2.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

For certificates issued by the Federal Common Policy~~ Root~~ CA, failure to object to the renewal of the certificate or its contents constitutes acceptance of the certificate.

For all other CAs operating under this policy, no stipulation.

4.6.6. Publication of the Renewal Certificate by the CA

~~As specified in section 2.1, ~~All CA certificates ~~shall~~must be published ~~in repositories~~as specified in Section 4.4.2.

This policy makes no stipulation regarding publication of Subscriber certificates, except as noted in Section 9.4.3.

4.6.7. Notification of Certificate Issuance by the CA to Other Entities

~~No stipulation.~~

As specified in Section 4.4.3.

4.7. Certificate Re-key

Re-~~keying a ~~key is identical to renewal except the new certificate ~~consists of creating new certificates with~~must have a different subject public key ~~(~~and serial number~~) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key. Re-key of a certificate does not require a change to the subjectName and does not violate the requirement for name uniqueness. ~~.

Once re-keyed, the old certificate may or may not be revoked, but must not be reused for requesting further renewals, re-~~keyed, renewed~~keys, or ~~modified~~modifications.

~~Subscribers shall identify themselves for the purpose of re-keying as required in section 3.3.~~

4.7.1. Circumstance for Certificate Re-key

~~The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a subscriber periodically obtain new keys. (Section 6.3.2 establishes usage periods for private keys for both CAs and subscribers.) Examples of~~ Circumstances requiring certificate re-key include~~:~~ nearing the maximum usage period of a private key, certificate expiration, loss or compromise, issuance of a new hardware token, and hardware token failure.

Section 6.3.2 establishes maximum usage periods for private keys for both CAs and Subscribers.

4.7.2. Who May Request Certification of a New Public Key

~~Requests for certification of a new public~~ For CA certificates and Delegated OCSP responder certificates, the corresponding operating authority may request re-key ~~shall be considered as follows:~~of its own certificate.

Subscribers with a currently valid certificate may request ~~certification of a new public~~ re-key~~.~~ of the certificate. CAs and RAs may request certification of a new public key on behalf of a Subscriber. ~~For device certificates,~~ The human sponsor of a device may request re-key of the device ~~may request certification of a new public key~~certificate.

4.7.3. Processing Certificate Re-keying Requests

~~Digital signatures on~~Subscribers must identify themselves for the purpose of re-keying as required in Section 3.3.

The CA or RA must verify the information provided prior to issuing the new certificate as specified in Section 4.3.

Digitally signed Subscriber re-key requests ~~shall~~must be validated before ~~electronic~~the re-key requests are processed.~~ Alternatively, subscriber re-key requests may be processed using the same process used for initial certificate issuance.~~

4.7.4. Notification of New Certificate Issuance to Subscriber

~~No stipulation.~~

As specified in Section 4.3.2.

4.7.5. Conduct Constituting Acceptance of a Re-keyed Certificate

For certificates issued by the Federal Common Policy~~ Root~~ CA, failure to object to the certificate or its contents constitutes acceptance of the certificate.

For all other CAs operating under this policy, no stipulation.

4.7.6. Publication of the Re-keyed Certificate by the CA

All CA certificates must be published as specified in Section 4.4.2~~.1~~.

~~This policy makes no stipulation regarding publication of subscriber certificates, except as noted in section 9.4.3.~~

This policy makes no stipulation regarding publication of Subscriber certificates, except as noted in Section 9.4.3.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

As specified in Section 4.4.3.

~~4.7.7.1.1.1. Notification of Certificate Issuance by the CA to Other Entities~~

~~No stipulation.~~

4.8. *Certificate Modification*

Modifying a certificate means creating a new certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old certificate. Once modified, the old certificate may or may not be revoked, but must not be reused for requesting further renewals, re-~~keyed, renewed~~keys, or ~~modified~~modifications.

4.8.1. Circumstance for Certificate Modification

~~A~~ CA ~~operating under this policy may modify a CA or~~certificates and Delegated OCSP responder ~~certificate~~certificates whose characteristics have changed (e.g. assert new policy OID~~).~~) may be modified. The new certificate may have the same or a different subject public key.

A ~~CA may perform~~ certificate ~~modification for~~associated with a Subscriber whose characteristics have changed (e.g., name change due to marriage~~).~~) may be modified. The new certificate ~~shall~~must have a different subject public key.

4.8.2. Who May Request Certificate Modification

~~Requests for certification of a new public key shall be considered as follows:~~ For CA certificates and Delegated OCSP responder certificates, the corresponding operating authority may request modification.

Subscribers with a currently valid certificate may request modification of the certificate. The human sponsor of a device may request modification of the device certificate. CAs and RAs may request certificate modification on behalf of a Subscriber. ~~For device certificates, the human sponsor of the device may request certificate modification.~~

4.8.3. Processing Certificate Modification Requests

~~If an individual's~~ Proof of all subject information changes (e.g., name changes ~~(e.g.,~~ due to marriage~~), then proof of the name change~~) must be provided to the RA or other designated agent ~~in order for a~~ .

The CA or RA must verify the information provided prior to issuing the new certificate ~~with the new name to be issued.~~ as specified in Section 4.3.

If an individual's authorizations or privileges change, ~~the RA will verify those~~ such that the modified certificate indicates a reduction in privileges and authorizations~~. If authorizations have reduced~~, the old certificate must be revoked.

~~Proof of all subject information changes must be provided to the RA or other designated agent and verified before~~If the modified certificate is issued with a new (different) public key, the additional requirements specified in Section 4.7.3 must also apply.

4.8.4. Notification of New Certificate Issuance to Subscriber

~~No stipulation.~~

As specified in Section 4.3.2.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

For certificates issued by the Federal Common Policy~~ Root~~ CA, failure to object to the certificate or its contents constitutes acceptance of the certificate.

For all other CAs operating under this policy, no stipulation

4.8.6. Publication of the Modified Certificate by the CA

All CA certificates must be published as specified in Section 4.4.2~~.1~~.

This policy makes no stipulation regarding publication of Subscriber certificates, except as noted in Section 9.4.3.

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

As specified in Section 4.4.3.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

~~This policy makes no stipulation regarding publication of Subscriber certificates, except as noted in Section 9.4.3.~~

~~4.8.7.1.1.1. Notification of Certificate Issuance by the CA to Other Entities~~

~~No stipulation.~~

~~4.9.1.1. CERTIFICATE REVOCATION AND SUSPENSION~~

~~CAs operating under this policy shall issue CRLs covering all unexpired certificates issued under this policy except for OCSP responder certificates that include the id-pkix-ocsp-nocheck extension.~~

~~CAs operating under this policy shall make public a description of how to obtain revocation information for the certificates they publish, and an explanation of the consequences of using dated revocation information. This information shall be given to subscribers during certificate request or issuance, and shall be readily available to any potential relying party.~~

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's public key, regardless of whether or not the associated private key has been compromised.

~~Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised.~~

Certificate suspension for CA certificates is ~~not allowed~~prohibited by this policy. However, the use of certificate suspension for ~~end entity~~Subscriber certificates is ~~allowed~~permitted.

For CAs operating under this policy, the FPKIPA ~~shall~~must be notified at least two weeks prior to the revocation of a CA certificate, whenever possible. For emergency revocation, CAs ~~shall~~must follow the notification procedures in Section 5.7.

4.9.1. Circumstances for Revocation

A certificate ~~shall~~must be revoked when the binding between the subject and the subject's public key defined within the certificate is no longer considered valid. Examples of circumstances that invalidate the binding are~~—~~:

- Identifying information or affiliation components of any names in the certificate becomes invalid. ~~This would~~ Examples include~~ evidence that~~ :
    - Subscriber no longer affiliated with sponsoring agency
    - A wild card certificate has been issued with a name where PKI Sponsor does not exercise control of the entire ~~name space~~namespace associated with the wild card certificate.
- Privilege attributes asserted in the Subscriber's certificate are reduced.
- The Subscriber can be shown to have violated the stipulations of its Subscriber agreement.
- There is reason to believe the private key has been compromised.
- The Subscriber or other authorized party (as defined in the CPS) asks for his/her certificate to be revoked.
- The failure of a CA to adequately adhere to the requirements of this CP or the approved CPS. ~~For example, there is strong evidence that the CA has failed to comply with the requirements of section 6.7 of the CP.~~

If it is determined that revocation is required, the associated certificate ~~shall~~must be revoked and placed on the CRL. Revoked certificates ~~shall~~must be included on all new publications of the certificate status information until the certificates expire.

If it is determined that a private key used to authorize the issuance of one or more certificates may have been compromised, all certificates directly or indirectly authorized by that private key since the date of actual or suspected compromise ~~shall~~must be revoked or ~~shall~~must be verified as appropriately issued.

4.9.2. Who Can Request Revocation

~~Within the PKI,~~ A CA may summarily revoke certificates ~~within its domain.~~it has issued. A written notice and brief explanation for the revocation ~~shall~~must subsequently be provided to the Subscriber. ~~The RA can request the revocation of a subscriber's certificate on behalf of any authorized party as specified in the CPS. A subscriber may request that its own certificate be revoked. The human~~

A Subscriber or sponsor of ~~a~~ device ~~can~~certificates may request ~~the~~ revocation of ~~the device's certificate.~~their own certificates.

The RA or other authorized agency officials may request the revocation ~~as described in the CPS.~~of a Subscriber's certificate.

The CA ~~shall~~must provide Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected private key compromise, certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to certificates. The CA ~~shall~~must publicly disclose the instructions through a readily accessible online means.

The FPKIPA can request revocation of any CA certificate issued under this CP.

4.9.3. Procedure for Revocation Request

A request to revoke a certificate ~~shall~~must identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). The steps involved in the process of requesting a ~~certification~~certificate revocation ~~are~~must be detailed in the CPS.

Where Subscribers use hardware tokens, revocation is optional if all the following conditions are met:

- the revocation request was not for key compromise;
- the hardware token does not permit the ~~user~~Subscriber to export the signature private key;
- the Subscriber ~~surrendered~~surrenders the token to ~~the PKI;~~an authorized individual (e.g. supervisor, human resources, RA, or CA representative);
- the token was zeroized or destroyed promptly upon surrender;
- the token has been protected from malicious use between surrender and zeroization or destruction.

In all other cases, revocation of the certificates is mandatory. Even where all the above conditions have been met, revocation of the associated certificates is recommended.

4.9.4. Revocation Request Grace Period

There is no grace period for revocation under this policy.

4.9.5. Time within which CA must Process the Revocation Request

CAs will revoke certificates as quickly as practical upon receipt of a ~~proper~~ revocation request. Revocation requests ~~shall~~must be processed before the next ~~CRL is published~~required CRL issuance as specified in Section 4.9.7, excepting those requests received within two hours of the next required CRL issuance. Revocation requests received within two hours of CRL issuance ~~shall~~must be processed before the following CRL is published.

The CA must maintain a continuous 24x7 ability to respond internally to high-priority problem reports, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a certificate that is the subject of such a complaint.

4.9.6. Revocation Checking Requirements for Relying Parties

~~No stipulation.~~

> ~~Practice note: Use of revoked certificates could have damaging or catastrophic consequences. The matter of how often new revocation data should be obtained is a determination to be made by the relying party, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.~~

Relying parties are expected to verify the validity of certificates as specified in [RFC 5280].

> Practice note: Use of revoked certificates could have damaging or catastrophic consequences. The matter of how often new revocation data should be obtained is a determination to be made by the relying party, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

4.9.7. CRL Issuance Frequency

CRLs ~~shall~~must be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below.

Certificate status information ~~shall~~must be published not later than the next scheduled update. This will facilitate the local caching of certificate status information for off-line or remote ~~(laptop)~~ operation.

	Maximum Interval for Routine CRL Issuance			
	Online CA		Offline CA*	
	Interval	nextUpdate	Interval	nextUpdate
Shared Service Provider CAs	18 hours	48 hours	35 days	37 days
All other CAs	18 hours	180 hours	35 days	37 days

*An offline CA may incorporate locally attached network equipment such as an HSM or storage array. The CA system and any such locally attached network equipment must be completely isolated (air-gapped) from all other networks and computing systems. With the exception of

Content Signers, offline CAs must not issue certificates to Subscribers, as defined in Section 1.3.4.

Circumstances related to emergency CRL issuance are specified in Section 4.9.12.

4.9.8. Maximum Latency for CRLs

~~CAs operating as part of the Shared Service Providers program that only issue certificates to CAs and that operate off-line must issue CRLs at least once every 24 hours, and the *nextUpdate* time in the CRL may be no later than 48 hours after issuance time (i.e., the *thisUpdate* time). Legacy Federal PKIs, root CAs, and the Common Policy Root CA that only issue certificates to CAs and that operate off-line must issue CRLs at least once every 31 days, and the *nextUpdate* time in the CRL may be no later than 32 days after issuance time (i.e., the *thisUpdate* time).~~

~~CAs that issue certificates to subscribers or operate on-line must issue CRLs at least once every 18 hours, and the *nextUpdate* time in the CRL may be no later than 48 hours after issuance time (i.e., the *thisUpdate* time). For legacy Federal PKIs only, the *nextUpdate* time in the CRL may be no later than 180 hours after issuance time (i.e., the *thisUpdate* time).~~

~~Practice Note: Since many applications only check for a new CRL at nextUpdate, a longer nextUpdate time may result in applications continuing to rely on older CRLs even when a newer CRL is available. A longer nextUpdate time also increases the potential of a replay attack to validate a newly revoked certificate. Where the CRL nextUpdate exceeds 48 hours, relying parties should consider these risks and take appropriate measures to mitigate the risk. For high-risk, sensitive Relying Party applications suggested measures include configuring a preference for OCSP by applications, pre-fetching CRLs at least every 18 hours, and use of other compensating controls.~~

~~Circumstances related to emergency CRL issuance are specified in Section 4.9.12.~~

~~4.9.8.1.1.1. Maximum Latency for CRLs~~

For CAs that operate online, CRLs ~~shall~~must be published within 4 hours of generation.

For CAs that operate offline, pre-generated CRLs intended for publication more than 4 hours after generation must be protected in the same manner as the CA. All pre-generated CRLs not yet published must be securely destroyed whenever the CA revokes any certificate. The CPS must describe protections and processes used for generation and protection of any pre-generated CRLs.

Furthermore, each CRL ~~shall~~must be published no later than the time specified in the nextUpdate field of the previously issued CRL~~ for same scope~~.

Note: If pre-generation of CRLs is implemented, the thisUpdate field will be the date of generation and the nextUpdate value will be no more than 37 days beyond the date of planned publication.

4.9.9. On-line Revocation/Status Checking Availability

~~4.9.9.1.1.1. On-line Revocation/Status Checking Availability~~

CAs ~~shall~~must support on-line status checking via OCSP [RFC 6960] for ~~end entity certificates issued under id-fpki-common-authentication, id-fpki-common-pivi-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-derived-pivAuth, id-fpki-common-cardAuth,~~Subscriber certificates. Since some relying parties cannot accommodate on-line communications, all CAs must support CRLs.

OCSP services must be designed and implemented so as to provide 99% availability overall and ~~id-fpki-common-pivi-cardAuth.~~ limit scheduled down-time to 0.5% annually, with resources sufficient to provide a response time of ten (10) seconds or less under normal operating conditions.

~~Where on-line status checking is supported,~~ Certificate status information ~~must be updated and available to relying parties within 18 hours of certificate revocation.~~

~~Where on-line status checking is supported and a certificate issued under id-fpki-common-High is revoked for key compromise, the status information~~distributed via OCSP must be updated and available to relying parties ~~within 6 hours~~to meet or exceed the requirements for CRL issuance.

The CA ~~shall~~must operate and maintain its CRL ~~and OCSP~~ capability with resources sufficient to provide a response time of ten (10) seconds or less under normal operating conditions.

~~The CA shall maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.~~

~~The CA shall maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.~~

~~Since some relying parties cannot accommodate on-line communications, all CAs will be required to support CRLs.~~

4.9.10. On-line Revocation Checking Requirements

~~Relying party client software may optionally support~~ On-line revocation status checking~~. Client software using on-line~~ is optional for relying parties. For certificates where revocation status online checking ~~need~~is not ~~obtain or process~~available, CRLs~~.~~ must be used.

4.9.11. Other Forms of Revocation Advertisements Available

A CA may also use other methods to publicize the certificates it has revoked. Any alternative method must meet the following requirements:

- The alternative method must be described in the CA's approved CPS;
- The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified.

- The alternative method must meet the issuance and latency requirements for CRLs stated in Sections 4.9.7 and 4.9.8.

4.9.12. Special Requirements Related To Key Compromise

When a CA certificate is revoked a CRL must be issued within 18 hours of notification.

When a CA certificate issued under id-fpki-common-high is revoked or Subscriber certificate issued under id-fpki-common-high is revoked because of compromise~~,~~ or suspected compromise~~,~~ of a private key, a CRL must be issued within six (6) hours of notification.

4.9.13. Circumstances for Suspension

For CA certificates, suspension is not permitted.

~~For end entity certificates, no stipulation.~~

CAs may support certificate suspension and restoration for Subscriber certificates. If suspension and restoration are supported by the CA, the CPS must describe under what circumstances and details for the corresponding sections below.

4.9.14. Who Can Request Suspension

No stipulation for ~~end entity~~Subscriber certificates.

4.9.15. Procedure for Suspension Request

No stipulation for ~~end entity~~Subscriber certificates.

4.9.16. Limits on Suspension Period

No stipulation for ~~end entity~~Subscriber certificates.

4.10. CERTIFICATE STATUS SERVICES

~~No stipulation.~~

See Section 4.9.9 for OCSP.

If additional certificate status services are supported, they must be described in the CPS.

4.10.1. Operational Characteristics

~~No stipulation.~~

Where applicable this must be described in the CPS.

4.10.2. Service Availability

~~No stipulation.~~

Where applicable this must be described in the CPS.

4.10.3. Optional Features

~~No stipulation.~~

Where applicable this must be described in the CPS.

4.11. End Of Subscription

No stipulation.

4.12. Key Escrow and Recovery

4.12.1. Key Escrow and Recovery Policy and Practices

CA private keys are never escrowed.

Human Subscriber key management keys ~~shall~~must be escrowed to provide key recovery. CAs ~~shall~~must develop a Key Recovery Practice Statement (KRPS) describing the procedures and controls implemented to comply with the FPKI Key Recovery Policy. The KRPS may be a separate document or may be combined with the appropriate Certification Practice Statement and/or Registration Practice Statement. The Federal PKI Policy Authority (FPKIPA) will determine the KRPS compliance with the KRP and this CP.

Under no circumstances ~~shall~~must a Subscriber signature key be held in trust by a third party.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

CAs that support session key encapsulation and recovery ~~shall~~must identify the document describing the practices in the applicable CPS.

5. Facility, Management, and Operational Controls

5.1. Physical Controls

CA equipment ~~shall~~must be protected from unauthorized access while the cryptographic module is installed and activated. The CA ~~shall~~must implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. CA cryptographic tokens ~~shall~~must be protected against theft, loss, and unauthorized use.

All the physical control requirements specified below apply equally to ~~the Common Policy Root CA and subordinate~~all CAs, and any remote workstations used to administer the CAs except where specifically noted.

Practice Note: The phrase “remote workstations used to administer the CAs,” refers to dedicated systems solely used for accessing either the system hosting the CA or the CA itself through external networks for maintenance and administration. It does not refer to administration workstations or consoles within the CA’s security perimeter or to Registration Authority workstations used by RAs to support certificate management and Subscribers.

5.1.1. Site Location and Construction

The location and construction of the facility housing the CA equipment, as well as sites housing remote workstations used to administer the CAs, ~~shall~~must be consistent with facilities used to house high-value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, ~~shall~~must provide robust protection against unauthorized access to the CA equipment and records.

5.1.2. Physical Access

5.1.2.1. Physical Access for CA Equipment

At a minimum, the physical access controls for CA equipment, as well as remote workstations used to administer the CAs, ~~shall —~~must:

- Ensure that no unauthorized access to the hardware is permitted.
- Ensure that all removable media and paper containing sensitive plain-text information is stored in secure containers.
- Be manually or electronically monitored for unauthorized intrusion at all times.
- Ensure an access log is maintained and inspected periodically.
- Require two-person physical access control to both the cryptographic module and computer systems.

When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, and CA equipment ~~shall~~must be placed in secure containers. Activation data ~~shall~~must be either memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and ~~shall~~must not be stored with the cryptographic module or removable hardware associated with remote workstations used to administer the CA.

A security check of the facility housing the CA equipment or remote workstations used to administer the CAs ~~shall~~must occur if the facility is to be left unattended. At a minimum, the check ~~shall~~must verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “open,” and secured when “closed,” and for the CA, that all equipment other than the repository is shut down).
- Any security containers are properly secured.
- Physical security systems (e.g., door locks, vent covers) are functioning properly.
- The area is secured against unauthorized access.

A person or group of persons ~~shall~~must be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance ~~shall~~must be maintained. If the facility is not continuously attended, the last person to depart ~~shall~~must initial a sign-out sheet that indicates the date and time and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.2.2. Physical Access for RA Equipment

RA equipment ~~shall~~must be protected from unauthorized access while the cryptographic module is installed and activated. The RA ~~shall~~must implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms ~~shall~~must be commensurate with the level of threat in the RA equipment environment.

5.1.2.3. Physical Access for CSS Equipment

Physical access control requirements for CSS equipment ~~(if implemented), shall~~that has signing capability must meet the CA physical access requirements specified in Section 5.1.2.1. CSS equipment that do not have a private signing key and only distribute pre-generated OCSP responses are not required to meet these requirements.

5.1.3. Power and Air Conditioning

The CA ~~shall~~must have ~~backup capability~~ sufficient ~~to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of~~ alternative power supply in the event of a primary power source failure to either maintain CA operations or ~~air conditioning causes a shutdown.~~, at a minimum, prevent loss of data. The repositories (containing CA certificates ~~and~~, CRLs~~) shall~~, and pre-generated OCSP responses) must be provided with uninterrupted power sufficient for a minimum of six (6) hours operation in the absence of commercial power, to maintain availability and avoid denial of service.

5.1.4. Water Exposures

CA equipment ~~shall~~must be installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors).

Potential water damage from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.

5.1.5. Fire Prevention and Protection

~~No stipulation.~~

The CA must comply with local commercial building codes for fire prevention and protection.

5.1.6. Media Storage

Media ~~shall~~must be stored so as to protect them from accidental damage (e.g., water, fire, or electromagnetic) and unauthorized physical access.

5.1.7. Waste Disposal

Sensitive media and documentation that are no longer needed for operations ~~shall~~must be destroyed in a secure manner. For example, sensitive paper documentation ~~shall~~must be shredded, burned, or otherwise rendered unrecoverable.

5.1.8. Off-Site Backup

~~Full system~~CA backups sufficient to recover from system failure ~~shall~~must be made on a periodic schedule, and described in a CA's CPS. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy ~~shall~~must be stored at an off-site location (separate from CA equipment). Only the latest full backup need be retained. The backup ~~shall~~must be stored at a site with physical and procedural controls commensurate to that of the operational CA.

For ~~legacy Federal PKIs operating an~~ offline ~~CA~~CAs, the ~~full system~~ backup ~~shall~~must be performed each time the system is turned on or once ~~a~~per week, whichever is less frequent.

Requirements for CA private key backup are specified in Section 6.2.4.1.

5.2. *PROCEDURAL CONTROLS*

5.2.1. Trusted Roles

A Trusted Role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The ~~people~~personnel selected to fill these roles must be extraordinarily responsible, or the integrity of the CA will be weakened. The functions performed in these roles form the basis of trust for the entire PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

The requirements of this policy are defined in terms of four roles~~. (Note: the information derives from the Certificate Issuing and Management Components (CIMC) Protection Profile.)~~, implementing organizations may define additional roles provided the following separation of duties are enforced.

1. Administrator – authorized to install, configure, and maintain the CA; establish and maintain system accounts; configure audit parameters; and generate PKI component keys.
2. Officer – authorized to request or approve certificate issuance and revocations.
3. Auditor – authorized to review, maintain, and archive audit logs.
4. Operator – authorized to perform system backup and recovery.

Administrators do not issue certificates to Subscribers.

~~The roles required for each level of assurance are identified in Section 5.2.4.~~ These four roles are employed at the CA, RA, and CSS locations as appropriate. Separation of duties ~~shall~~must comply with Section 5.2.4, and requirements for two-person control with Section 5.2.2, regardless of the titles and numbers of Trusted Roles.

5.2.2. Number of Persons Required per Task

Two or more persons are required for the following tasks:

- CA key generation;
- CA signing key activation;
- CA private key backup.

Where multiparty control is required, at least one of the participants ~~shall~~must be an Administrator. All participants must serve in a Trusted Role as defined in Section 5.2.1. Multiparty control ~~shall~~must not be achieved using personnel that serve in the Auditor Trusted Role.

5.2.3. Identification and Authentication for Each Role

An individual ~~shall~~must identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

5.2.4. Roles Requiring Separation of Duties

Individuals may only assume one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. The CA and RA software and hardware ~~shall~~must identify and authenticate its users and ~~shall~~must ensure that no user identity can assume both the Administrator and Officer roles, assume both the Administrator and Auditor roles, or assume both the Auditor and Officer roles. For CAs that issue at id-fpki-common-high, the Auditor may not assume any other role. No individual ~~shall~~must have more than one identity.

5.3. *PERSONNEL CONTROLS*

5.3.1. Qualifications, Experience, and Clearance Requirements

All persons filling Trusted Roles ~~shall~~must be selected on the basis of loyalty, trustworthiness, and integrity, and must be U.S. citizens. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the CA ~~shall~~must be set forth in the CPS.

The FPKIMA Program Manager must hold a Top Secret security clearance.

5.3.2. Background Check Procedures

CA personnel ~~shall, at~~must receive a ~~minimum, pass~~favorable adjudication after undergoing a background investigation covering the following areas:

- Employment;
- Education;
- Place of residence;
- Law Enforcement; and
- References.

The period of investigation must cover at least the last five years for each area, excepting the residence check which must cover at least the last three years. Regardless of the date of award, the highest educational degree ~~shall~~must be verified.

Adjudication of the background investigation ~~shall~~must be performed by a competent adjudication authority using a process consistent with [Executive Order 12968~~ August 1995,~~], or equivalent.

5.3.3. Training Requirements

All personnel performing duties with respect to the operation of the CA or RA ~~shall~~must receive comprehensive training. Training ~~shall~~must be conducted in the following areas:

- CA (or RA) security principles and mechanisms;
- All PKI software versions in use on the CA (or RA) system;
- All PKI duties they are expected to perform;
- Disaster recovery and business continuity procedures; and
- Stipulations of this policy and appropriate CPS.

5.3.4. Retraining Frequency and Requirements

All individuals responsible for PKI roles ~~shall~~must be made aware of changes in the CA operation. Any significant change to the operations ~~shall~~must have a training (awareness) plan, and the execution of such plan ~~shall~~must be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

Documentation ~~shall~~must be maintained identifying all personnel who received training and the level of training completed.

5.3.5. Job Rotation Frequency and Sequence

~~No stipulation.~~

Job rotation must not violate role separation. All access rights associated with a previous role must be terminated.

All job rotations must be documented. Individuals assuming an auditor role must not audit their own work from a previous role.

5.3.6. Sanctions for Unauthorized Actions

The CA ~~shall~~must take appropriate administrative and disciplinary actions against personnel who have performed actions involving the CA or its RAs that are not authorized in this CP, CPSs, or other published procedures.

5.3.7. Independent Contractor Requirements

Contractors fulfilling Trusted Roles are subject to all personnel requirements stipulated in this policy.

PKI vendors who provide any services ~~shall~~must establish procedures to ensure that any subcontractors perform in accordance with this policy and the CPS.

5.3.8. Documentation Supplied to Personnel

Documentation sufficient to define duties and procedures for each role ~~shall~~must be provided to the personnel filling that role.

5.4. *AUDIT LOGGING PROCEDURES*

Audit log files ~~shall~~must be generated for all events relating to the security of the CA. For CAs operated in a virtual machine environment (VME)[3], audit logs ~~shall~~must be generated for all applicable events on both the virtual machine (VM) and isolation kernel (i.e. hypervisor).

Where possible, the security audit logs ~~shall~~must be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism ~~shall~~must be used. All security audit logs, both electronic and non-electronic, ~~shall~~must be retained and made available during compliance audits.

5.4.1. Types of Events Recorded

All security auditing capabilities of CA operating system and CA applications required by this CP ~~shall~~must be enabled during installation. At a minimum, each audit record ~~shall~~must include the following (either recorded automatically or manually for each auditable event):

- The type of event;
- The date and time the event occurred;
- A success or failure indicator when executing the CA's signing process;
- A success or failure indicator when performing certificate revocation; and
- The identity of the entity and/or operator that caused the event.

A message from any source requesting an action requiring the use of a private key controlled by the CA is an auditable event; the corresponding audit record must also include message date and time, source, destination, and contents.

The CA ~~shall~~must record ~~the~~ events identified in the list below. Where these events cannot be electronically logged, ~~the CA shall supplement~~ electronic audit logs must be supplemented with physical logs as necessary~~:~~..

- SECURITY AUDIT:
  - Any changes to the Audit parameters, e.g., audit frequency, type of event audited
  - Any attempt to delete or modify the Audit logs
  - Obtaining a third-party time-stamp
- IDENTIFICATION AND AUTHENTICATION:
  - Successful and unsuccessful attempts to assume a role

[3] For the purposes of this policy, the definition of a virtual machine environment does not include cloud-based solutions (e.g. platform-as-a-service) or container-type solutions (e.g. Docker), which are not permitted for any CA operating under this policy.

  - The value of maximum authentication attempts is changed
  - Maximum authentication attempts unsuccessful authentication attempts occur during user login
  - An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
  - An Administrator changes the type of authenticator, e.g., from password to biometrics
- LOCAL DATA ENTRY:
  - All security-relevant data that is entered in the system
- REMOTE DATA ENTRY:
  - All security-relevant messages that are received by the system
- DATA EXPORT AND OUTPUT:
  - All successful and unsuccessful requests for confidential and security-relevant information
- KEY GENERATION:
  - Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)
- PRIVATE KEY LOAD AND STORAGE:
  - The loading of Component private keys
  - All access to certificate subject private keys retained within the CA for key recovery purposes
- TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE:
  - All changes to the trusted public keys, including additions and deletions
- SECRET KEY STORAGE:
  - The manual entry of secret keys used for authentication
- PRIVATE AND SECRET KEY EXPORT:
  - The export of private and secret keys (keys used for a single session or message are excluded)
- CERTIFICATE REGISTRATION:
  - All certificate requests
- CERTIFICATE REVOCATION:
  - All certificate revocation requests
- CERTIFICATE STATUS CHANGE APPROVAL:
  - The approval or rejection of a certificate status change request
- CA CONFIGURATION:
  - Any security-relevant changes to the configuration of the CA

- ACCOUNT ADMINISTRATION:
  - Roles and users are added or deleted
  - The access control privileges of a user account or a role are modified
- CERTIFICATE PROFILE MANAGEMENT:
  - All changes to the certificate profile
- REVOCATION PROFILE MANAGEMENT:
  - All changes to the revocation profile
- CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT:
  - All changes to the certificate revocation list profile
- MISCELLANEOUS:
  - Appointment of an individual to a trusted role
  - Designation of personnel for multiparty control
  - Installation of the operating system
  - Installation of the CA
  - Installing hardware cryptographic modules
  - Removing hardware cryptographic modules
  - Destruction of cryptographic modules
  - System startup
  - Logon attempts to CA applications
  - Receipt of hardware / software
  - Attempts to set passwords
  - Attempts to modify passwords
  - Backing up CA internal database
  - Restoring CA internal database
  - File manipulation (e.g., creation, renaming, moving)
  - Posting of any material to a repository
  - Access to CA internal database
  - All certificate compromise notification requests
  - Loading tokens with certificates
  - Shipment of tokens
  - Zeroizing tokens
  - Re-key of the CA
  - Configuration changes to the CA server involving:
    - Hardware
    - Software

        - Operating system
        - Patches
        - Security profiles
- PHYSICAL ACCESS / SITE SECURITY:
    - Personnel access to room housing CA
    - Access to the CA server
    - Known or suspected violations of physical security
- ANOMALIES:
    - Software error conditions
    - Software check integrity failures
    - Receipt of improper messages
    - Misrouted messages
    - Network attacks (suspected or confirmed)
    - Equipment failure
    - Electrical power outages
    - Uninterruptible power supply (UPS) failure
    - Obvious and significant network service or access failures
    - Violations of certificate policy
    - Violations of certification practice statement
    - Resetting operating system clock

5.4.2. Frequency of Processing Log

For CAs that issue certificates under id-fpki-common-high, ~~review of~~ the audit log ~~shall~~must be ~~required~~reviewed at least once every month. For CAs that do not issue certificates under id-fpki-common-high, ~~review of~~ the audit log ~~shall~~must be ~~required~~reviewed at least once every two months.

Such reviews ~~involve verifying~~may be performed manually or by an automated process, and must include verification that the ~~log has~~logs have not been tampered with ~~and then briefly inspecting all~~, an inspection of log entries, ~~with~~and a ~~more thorough investigation of~~root cause analysis for any alerts or irregularities ~~in the logs~~. A statistically significant portion of the security audit data generated by the CA since the last review ~~shall~~must be examined. This amount will be described in the CPS.

All significant events ~~shall~~must be explained in an audit log summary. Actions taken as a result of these reviews ~~shall~~must be documented.

5.4.3. Retention Period for Audit Log

Audit logs ~~shall~~must be retained on-site until reviewed, in addition to being archived as described in Section 5.5. ~~The individual who removes audit logs from the CA system shall be an official different from the individuals who, in combination, command the CA signature key.~~

5.4.4. Protection of Audit Log

~~The security audit data shall not be open for reading or modification by any human, or by any automated process, other than those that perform security audit processing. CA system~~ System configuration and operational procedures must be implemented together to ensure that:

- Only authorized ~~people~~individuals and systems have read access to the logs;
- Only authorized auditors may archive ~~or delete security~~ audit ~~data.~~ logs; and,
- Audit logs are not modified.

Collection of the audit logs from the CA system must be performed by, witnessed by or under the control of trusted roles who are different from the individuals who, in combination, command the CA signature key.

For RA, the authorized individual must be a system administrator other than the RA.

Procedures must be implemented to protect archived data from deletion or destruction before the end of the security audit data retention period (note that deletion requires modification access). Security audit data ~~shall~~must be moved to a safe, secure storage location separate from the location where the data was generated.

5.4.5. Audit Log Backup Procedures

Audit logs and audit summaries ~~shall~~must be backed up at least monthly. A copy of the audit log ~~shall~~must be sent off-site on a monthly basis.

5.4.6. Audit Collection System (Internal vs. External)

The audit log collection system may or may not be external to the CA system. Automated audit processes ~~shall~~must be invoked at system or application startup, and cease only at system or application shutdown. Audit collection systems ~~shall~~must be configured such that security audit data is protected against loss (e.g., overwriting or overflow of automated log files). ~~Should it become apparent that~~If an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, operations ~~shall~~must be suspended until the problem has been remedied.

5.4.7. Notification to Event-Causing Subject

There is no requirement to notify a subject that an event was audited. Real-time alerts are neither required nor prohibited by this policy.

5.4.8. Vulnerability Assessments

~~The CA will~~CAs must perform routine self-assessments of security controls.

~~Practice Note: The security audit data should be reviewed by the security auditor for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. Security auditors should check for continuity of the security audit data.~~

Practice Note: The security audit data should be reviewed by the security auditor for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. Security auditors should check for continuity of the security audit data.

5.5. Records Archival

~~The Common Policy CA~~CAs must follow either the General Records Schedules established by the National Archives and Records Administration or an agency-specific schedule as applicable.

5.5.1. Types of Events Archived

CA archive records ~~shall~~must be sufficiently detailed to determine the proper operation of the CA and the validity of any certificate (including those revoked or expired) issued by the CA. At a minimum, the following data ~~shall~~must be recorded for archive:

- ~~CA accreditation (if applicable)~~
- CA Authority To Operate
- Certificate Policy
- Certification Practice Statement
- Contractual obligations and other agreements concerning operations of the CA
- System and equipment configuration
- Modifications and updates to system or configuration
- Certificate requests
- All certificates issued and/or published
- Record of re-key
- Revocation requests
- Subscriber identity authentication data as per Section 3.2.3
- Documentation of receipt and acceptance of certificates (if applicable)
- Subscriber agreements
- Documentation of receipt of tokens
- All CRLs issued and/or published
- Other data or applications to verify archive contents
- Compliance Auditor reports

- Any changes to the Audit parameters, e.g~~.~~., audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs
- Whenever the CA generates a key (not mandatory for single session or one-time use symmetric keys)
- All access to certificate subject private keys retained within the CA for key recovery purposes
- All changes to the trusted public keys, including additions and deletions
- The export of private and secret keys (keys used for a single session or message are excluded)
- The approval or rejection of a certificate status change request
- Appointment of an individual to a Trusted Role
- Destruction of cryptographic modules
- All certificate compromise notifications
- Remedial action taken as a result of violations of physical security
- Violations of Certificate Policy
- Violations of Certification Practice Statement

5.5.2. Retention Period for Archive

For CAs that issue certificates under id-fpki-common-high,~~ archive~~ records must be kept for a minimum of 20 years and 6 months without any loss of data.

For CAs that do not issue certificates under id-fpki-common-high,~~ archive~~ records must be kept for a minimum of 10 years and 6 months without any loss of data.

5.5.3. Protection of Archive

~~No unauthorized user shall be~~Only authorized users are permitted to write to, modify, or delete the archive. ~~For the CA, ~~Archived records may be moved to another medium. The contents of the archive ~~shall~~must not be released except in accordance with Sections 9.3 and 9.4.

~~Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. ~~Archive media ~~shall~~must be stored in a safe, secure storage facility geographically separate from the CA~~.~~

~~If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site.~~

~~Alternatively, a CA operating under this policy may retain data~~ using ~~whatever ~~procedures ~~have been ~~approved by NARA ~~for that category of documents.~~or according to agency-specific policy. Applications required to process the archive data ~~shall~~must be maintained for a period that equals or exceeds the archive requirements for the data.

~~Prior to the end of the archive retention period, the FPKIMA shall provide archived data and the applications necessary to read the archives to an FPKIPA-approved archival facility, which shall retain the applications necessary to read this archived data.~~

5.5.4. Archive Backup Procedures

No stipulation.

5.5.5. Requirements for Time-Stamping of Records

CA archive records ~~shall~~must be automatically time-stamped as they are created. The CPS ~~shall~~must describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

5.5.6. Archive Collection System (Internal or External)

Archive data may be collected in any expedient manner.

5.5.7. Procedures to Obtain and Verify Archive Information

Copies of records of individual transactions may be released upon request of any Subscribers involved in the transaction or their legally recognized agents.

Procedures, detailing how to create, verify, package, transmit, and store the CA archive information, ~~shall~~must be ~~published~~included in the CPS.

5.6. KEY CHANGEOVER

~~To minimize risk from compromise~~Each CA's signing key must have a validity period as described in Section 6.3.2.

Prior to the end of a CA's ~~private~~ signing~~ key, that~~ key ~~may~~ validity period, a new CA must be ~~changed often.~~established or a re-key on the existing CA must be performed. This is referred to as key changeover. From that time on, only the new key ~~will~~must be used to sign CA and Subscriber certificates. The old private key may continue to be used to sign CRLs and OCSP responder certificates. If the old private key is used to sign OCSP responder certificates or CRLs that cover certificates signed with that key, the old key must be retained and protected.

After ~~a CA performs a Key Changeover, the CA may continue to issue CRLs with the old key until~~ all certificates signed with ~~that~~the old key have expired~~. As an alternative, after all certificates signed with that old key have~~ or been revoked, the CA may issue a final long-term CRL using the old key, with a nextUpdate time past the validity period of all issued certificates. This final CRL ~~shall~~must be available for all relying parties until the validity period of all issued certificates has ~~past~~passed. Once the last CRL has been issued, the old private signing key of the CA may be destroyed.

~~The CA's signing key shall have a validity period as described in section 6.3.2.~~

When a CA ~~updates its private signature~~performs a key changeover and thus generates a new public key, the CA ~~shall~~must notify all CAs, RAs, and Subscribers that rely on the CA's certificate that it has been changed.

When a CA ~~that distributes self-signed certificates updates its private signature key~~performs a key changeover, the CA ~~shall~~may generate key rollover certificates, where the new public key is signed by the old private key, and vice versa. This permits immediate acceptance of newly issued certificates and CRLs ~~without distribution of the new self-signed certificate to~~by current users.~~ Key rollover certificates are optional for CAs that do not distribute self-signed certificates. SSPs and Federal Legacy PKIs CAs cross certified with the Common Policy Root CA must be able to continue to interoperate with the Common Policy Root CA after the Common Policy Root CA performs a key rollover, whether or not the DN of the Common Policy Root CA is changed.~~

5.7. COMPROMISE AND DISASTER RECOVERY

CAs under this policy must have an incident handling process, which documents any security incidents. Security incidents may include violation or threat of violation to the system, improper usage, malicious or anomalous activity and violations of the CPS or CP.

5.7.1. Incident and Compromise Handling Procedures

The FPKIPA ~~shall~~must be notified within 24 hours if any CAs operating under this policy experience the following:

- suspected or detected compromise of the CA systems;
- ~~suspected or detected compromise of a certificate status server (CSS) if (1) the CSS certificate has a lifetime of more than 72 hours and (2) the CSS certificate cannot be revoked (e.g., an OCSP responder certificate with the id-pkix-ocsp-nocheck extension);~~
- physical or electronic penetration of CA systems;
- successful denial of service attacks on CA components; ~~or~~
- any incident preventing the CA from issuing a CRL ~~within 48 hours of~~ prior to the ~~issuance~~nextUpdate time of the previous CRL~~.~~;

~~The FPKIPA will take appropriate steps to protect the integrity of the Federal PKI.~~

~~The CA's Management Authority shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the CA's CPS.~~

- ~~In the event~~suspected or detected compromise of a CSS; or
- suspected or detected compromise of an RA.

The notification must include preliminary remediation analysis.

Once the incident ~~as described above~~has been resolved, the organization operating the CA ~~shall notify the FPKIPA within 24 hours of incident discovery, along with preliminary remediation analysis.~~

~~Within 10 business days of incident resolution, the organization operating the CA shall post a notice on its publically available web page identifying the incident and~~must provide notification directly to the FPKIPA which includes detailed measures taken to remediate the incident. The ~~public~~ notice ~~shall~~must include the following:

1. Which CA components were affected by the incident
2. The CA's interpretation of the incident~~.~~
3. Who is impacted by the incident
4. When the incident was discovered
5. A complete list of all certificates that ~~were either~~may have been issued erroneously or are not compliant with the CP/CPS as a result of the incident
6. A statement that the incident has been fully remediated

~~The notification provided directly to the FPKIPA shall also include detailed measures taken to remediate the incident. The FPKIPA will post the notices to idmanagement.gov and provide an announcement to all Federal Agencies and Bridge Affiliate PKIs.~~

5.7.2. Computing Resources, Software, and/or Data Are Corrupted

When computing resources, software, and/or data are corrupted, CAs ~~operating under this policy shall~~must respond as follows:

- Before returning to operation, ensure that the system’s integrity has been restored.
- If the CA signature keys are not destroyed, CA operation ~~shall~~must be reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in Section 4.9.7.
- If the CA signature keys are destroyed, CA operation ~~shall~~must be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.

The customer Agency ~~PMA shall~~Points of Contact (POC) must be notified as soon as possible.

In the event of an incident as described above, the organization operating the CA ~~shall~~must post a notice on its web page identifying the incident and provide notification to the FPKIPA. See Section 5.7.1 for contents of the notice.

5.7.3. Entity (CA) Private Key Compromise Procedures

In the event of a CA private key compromise, the following operations must be performed~~.~~:

- The ~~FPKIPA shall be~~CA must immediately ~~informed, as well as any superior or cross-certified CAs~~inform the FPKIPA and any entities known to be distributing the CA certificate (e.g., in a root store).
- The CA must request revocation of any certificates issued to the compromised CA.
- The CA must generate new keys in accordance with Section 6.1.1.1.

If the CA distributed the ~~private~~public key in a Trusted Certificate, the CA ~~shall~~must perform the following operations:

- Generate a new Trusted Certificate.
- Securely distribute the new Trusted Certificate as specified in Section 6.1.4.
- Initiate procedures to notify Subscribers of the compromise.

Subscriber certificates issued prior to compromise of the CA private key may be renewed automatically by the CA under the new key pair (see Section 4.6~~),~~) or the CA may require Subscribers to repeat the initial certificate application process.

The organization operating the CA ~~shall~~must post a notice on its web page describing the compromise. See Section 5.7.1 for contents of the notice.

5.7.4. Business Continuity Capabilities after a Disaster

For the Federal Common Policy ~~Root~~ CA, recovery procedures ~~shall~~must be in place to reconstitute the CA within six (6) hours of failure.

All other CAs operating under this policy ~~shall~~must have recovery procedures in place to reconstitute the CA within 72 hours of failure.

In the case of a disaster whereby the CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, the FPKIPA ~~shall~~must be notified at the earliest feasible time, and the FPKIPA ~~shall~~must take whatever action it deems appropriate.

~~Relying parties may decide of their own volition whether to continue to use certificates signed with the destroyed private key pending reestablishment of CA operation with new certificates.~~

5.8. CA OR RA TERMINATION

Whenever possible, the FPKIPA ~~shall~~must be notified at least two weeks prior to the termination of a CA operating under this policy. For emergency termination, CAs ~~shall~~must follow the notification procedures in Section 5.7.

When a CA operating under this policy terminates operations before all certificates have expired, the CA signing keys ~~shall~~must be surrendered to the FPKIPA. This Section does not apply to CAs that have ceased issuing new certificates but are continuing to issue CRLs until all certificates have expired. Such CAs are required to continue to conform with all relevant aspects of this policy (e.g., audit logging and archives).

Any issued certificates that have not expired, ~~shall~~must be revoked and a final long term CRL with a nextUpdate time past the validity period of all issued certificates ~~shall~~must be generated. This final CRL ~~shall~~must be available for all relying parties until the validity period of all issued certificates has ~~past.~~passed. Once the last CRL has been issued, the private signing key(s) of the CA to be terminated will be destroyed or taken offline, designated as “not in use”, and protected as stipulated in Section 5.1.2.1.

Prior to CA termination, the CA ~~shall~~must provide archived data to an archive facility as specified in the CPS. As soon as possible, the CA will advise all other organizations to which it has issued certificates of its termination, using an agreed-upon method of communication specified in the CPS.

When an organizational RA function operating under this policy terminates operations, the RA must archive all audit logs and other records prior to termination and destroy its private keys upon termination.

6. Technical Security Controls

6.1. *Key Pair Generation and Installation*

6.1.1. Key Pair Generation

6.1.1.1. CA Key Pair Generation

Cryptographic keying material used by CAs to sign certificates, CRLs or status information ~~shall~~must be generated in [FIPS 140] validated cryptographic modules~~. For CAs that issue certificates under id-fpki-common-High, the module(s) shall meet or exceed FIPS 140 Level 3. For CAs that do not issue certificates under id-fpki-common-High, the module(s) shall meet or exceed FIPS 140 Level ~~ as specified in Section 6.2.1. Multiparty control is required for CA key pair generation, as specified in Section 6.2.2.

CA key pair generation must create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure must be detailed enough to show that appropriate role separation was used. An independent third party ~~shall~~must validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

> ~~Practice Note: If the audit trail identifies and documents any failures or anomalies in the key generation process, along with the corrective action taken, the key generation process need not be restarted but may continue.~~

> Practice Note: If the audit trail identifies and documents any failures or anomalies in the key generation process, along with the corrective action taken, the key generation process need not be restarted but may continue.

6.1.1.2. Subscriber Key Pair Generation

Subscriber key pair generation may be performed by the Subscriber, CA, or RA. If the CA or RA generates Subscriber key pairs, the requirements for key pair delivery specified in Section 6.1.2 must also be met.

~~Validated software or hardware cryptographic modules shall be used to generate all subscriber key pairs, as well as pseudo-random numbers and parameters used in key pair generation. For the id-fpki-common-hardware, id-fpki-common-High, id-fpki-common-authentication, id-fpki-common-pivi-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-pivi-cardAuth, and id-fpki-common-cardauth policies, subscriber key pairs shall be generated in FIPS~~

~~140 Level 2 hardware cryptographic modules. Any pseudo-random numbers used for key generation material shall be generated by a FIPS-approved method. Symmetric keys may be generated by means of either software or hardware mechanisms.~~

> ~~Practice Note: If the audit trail identifies and documents any failures or anomalies in the key generation process, along with the corrective action taken, the key generation process need not be restarted but may continue.~~

Subscriber key pairs must be generated in [FIPS 140] validated cryptographic modules as specified in Section 6.2.1.

For PIV, all keys, with the exception of key management, must be generated on the card.

6.1.1.3. CSS Key Pair Generation

Cryptographic keying material used by ~~CSSes~~CSSs to sign status information ~~shall~~must be generated in [FIPS 140] validated cryptographic modules~~. For CSSes that provide status under id-fpki-common-High, the module(s) shall meet or exceed FIPS 140 Level 3. For CSSes that do not provide status under id-fpki-common-High, the module(s) shall meet or exceed FIPS 140 Level~~ as specified in Section 6.2.1.

6.1.1.4. PIV Content Signing Key Pair Generation

Cryptographic keying material used by PIV issuing systems or devices for Common PIV Content Signing ~~shall~~must be generated in [FIPS 140] validated cryptographic modules~~. For PIV issuing systems or devices that sign PIV objects on PIV cards that contain certificates that assert id-fpki-common-High, the module(s) shall meet or exceed FIPS 140 Level 3. For all other PIV issuing systems or devices, the module(s) shall meet or exceed FIPS 140 Level~~ as specified in Section 6.2.~~ Key generation procedures shall be documented.~~1.

6.1.2. Private Key Delivery to Subscriber

If Subscribers generate their own key pairs, then there is no need to deliver private keys, and this section does not apply.

When CAs or RAs generate keys on behalf of the Subscriber, then the private key must be delivered securely to the Subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements must be met:

- Anyone who generates a private signing key for a Subscriber ~~shall~~must not retain any copy of the key after delivery of the private key to the Subscriber.
- The private key(s) must be protected from activation, compromise, or modification during the delivery process.
- The Subscriber ~~shall~~must acknowledge receipt of the private key(s).
- Delivery ~~shall~~must be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers.

  - For hardware modules, accountability for the location and state of the module must be maintained until the Subscriber accepts possession of it.
  - For electronic delivery of private keys, the key material ~~shall~~must be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data ~~shall~~must be delivered using a separate secure channel.

The CA must maintain a record of the Subscriber acknowledgment of receipt of the token.

6.1.3. Public Key Delivery to Certificate Issuer

Where key pairs are generated by the Subscriber or RA, the public key and the Subscriber's identity must be delivered securely to the CA for certificate issuance. The delivery mechanism ~~shall~~must bind the Subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it must be at least as strong as the ~~CA keys used to sign the certificate~~Subscriber key pair.

6.1.4. CA Public Key Delivery to Relying Parties

~~When a CA updates its signature key pair, the CA shall distribute the new public key in a secure fashion. The new public key may be distributed in a self-signed certificate, in a key rollover certificate, or in cross-certificates.~~

~~Self-signed certificates shall~~The self-signed root CA certificates must be conveyed to relying parties in a secure fashion to preclude substitution attacks. Acceptable methods ~~for self-signed certificate delivery are~~include:

- ~~Loading a self-signed certificate onto tokens delivered to relying parties via secure mechanisms; such as~~
  - ~~The Trusted Certificate is loaded onto the token during the subscriber's appearance at the RA.~~
  - ~~The Trusted Certificate is loaded onto the token when the RA generates the subscriber's key pair and loads the private key onto the token, which is then delivered to the subscriber in accordance with section 6.1.2.~~
- Secure distribution of ~~self-signed certificates~~ the certificate through secure out-of-band mechanisms;
- Download the certificate from a Federal Government operated web site secured with a currently valid certificate and subsequent comparison of the hash of the ~~self-signed~~ certificate against a hash value made available via authenticated out-of-band sources (note that hashes posted in-band along with the certificate are not acceptable as an authentication mechanism~~); and~~)

- ~~Loading certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded.~~

~~Practice Note: Other methods that preclude substitution attacks may be considered acceptable.~~

~~Key rollover certificates are signed with the CA's current private key, so secure distribution is not required.~~

~~Practice Note: To ensure the availability of the new public key, the key rollover certificates must be distributed using repositories.~~

Practice Note: Other methods that preclude substitution attacks may be considered acceptable.

6.1.5. Key Sizes

This CP requires use of RSA PKCS #1, RSASSA-PSS, or ECDSA signatures; additional restrictions on key sizes and hash algorithms are detailed below. Certificates issued under this policy ~~shall~~must contain 2048, 3072, or 4096-bit RSA keys, or 256 or 384-bit elliptic curve ~~public keys~~keys. CAs that generate certificates and CRLs under this policy must use the SHA-256, SHA-384, or SHA-512 hash algorithm when generating digital signatures.

~~Practice Note: Future versions of this policy may specify additional FIPS-approved signature algorithms.~~

~~Trusted Certificates that expire before January 1, 2031 shall contain subject public keys of 2048 or 3072 bits for RSA or 256 or 384 bits for elliptic curve, and be signed with the corresponding private key. Trusted Certificates that expire on or after January 1, 2031 shall contain subject public keys of at least 3072 bits for RSA or 256 or 384 bits for elliptic curve, and be signed with the corresponding private key.~~

	~~Practice Note: Where certificates are issued to satisfy FIPS 201 requirements, CAs shall use signature keys of 2048 or 3072 or 4096 bits for RSA and 256 or 384 bits for elliptic curve algorithms to sign certificates issued on or after January 1, 2008.~~ CA certificates that expire on or before December 31, 2030	CA certificates that expire after December 31, 2030
Minimum Key Size	RSA: 2048 Elliptic Curve: 256	RSA: 3072 Elliptic Curve: 256
Hash Algorithm	SHA-256, SHA-384, or SHA-512	SHA-256, SHA-384, or SHA-512

~~CAs that generate certificates and CRLs under this policy shall use signature keys of 1024, 2048, 3072, or 4096 bits for RSA and 256 or 384 bits for elliptic curve algorithms. Certificates that~~

~~expire on or after December 31, 2010 shall be generated with 2048 or 3072 bit keys for RSA and 256 or 384 bit keys for elliptic curve algorithms. Certificates that expire after December 31, 2030 shall be generated with at least 3072 bit keys for RSA and 256 or 384 bit keys for elliptic curve algorithms.~~

~~CAs that generate certificates and CRLs under this policy shall use the SHA-1, SHA-256, or SHA-384 hash algorithm when generating digital signatures. RSA signatures on certificates and CRLs that are issued after December 31, 2010 shall be generated using SHA-256, however, RSA signatures on CRLs that are issued before January 1, 2012, and that include status information for certificates that were generated using SHA-1 may be generated using SHA-1. RSA signatures on CRLs that are issued on or after January 1, 2012, but before January 1, 2014 that only provide status information for certificates that were generated using SHA-1 may continue to be generated using SHA-1. ECDSA signatures on certificates and CRLs shall be generated using SHA-256 or SHA-384, as appropriate for the key length.~~

~~RSA signatures on certificates that are issued after December 31, 2010 and before January 1, 2014, to CAs that issued certificates prior to December 31, 2010 may be generated using SHA-1 provided that CA issues no additional end entity certificates. Additionally, certificates issued to OCSP responders that include SHA-1 certificates may be signed using SHA-1 until December 31, 2013. CAs that issue certificates signed with SHA-224 or SHA-256 after December 31, 2010 must not issue certificates signed with SHA-1.~~

~~Where implemented, CSSs shall sign responses using the same signature algorithm, key size, and hash algorithm used by the CA to sign CRLs. After December 31, 2010, OCSP responders that generate signatures on OCSP responses using SHA-1 shall only provide signed responses that are pre-produced (i.e., any signed response that is provided to an OCSP client shall have been signed before the OCSP responder received the request from the client).~~

~~End entity certificates issued under id-fpki-common-devices that expire before December 31, 2010 shall contain RSA public keys that are 1024, 2048, or 3072 bits in length or elliptic curve keys that are 256 or 384 bits. End entity certificates issued under id-fpki-common-devices and id-fpki-common-devicesHardware that expire on or after December 31, 2010 shall contain RSA public keys that are 2048 or 3072 bits or elliptic curve keys that are 256 or 384 bits. End entity certificates issued under id-fpki-common-devices and id-fpki-common-devicesHardware that expire after~~

	Subscriber certificates that expire on or before December 31, 2030	Subscriber certificates that expire after December 31, 2030
Minimum Key Size	RSA: 2048 Elliptic Curve: 256	RSA: 3072 Elliptic Curve: 256
Hash Algorithm	SHA-256, SHA-384, or SHA-512	SHA-256, SHA-384, or SHA-512

Practice Note: Future versions of this policy may specify additional FIPS-approved signature algorithms.

Practice Note: Reference NIST Special Publication 800-78 for algorithms and key sizes for certificates stored on PIV or Derived PIV credentials.

~~December 31, 2030 shall contain RSA public keys that are 3072 bits or elliptic curve keys that are 256 or 384 bits.~~

~~End entity certificates issued under id-fpki-common-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-derived-pivAuth, or id-fpki-common-cardAuth shall contain RSA public keys that are 2048 bits in length or elliptic curve keys that are 256 bits.~~

~~End entity certificates issued under id-fpki-common-policy, id-fpki-common-hardware, and id-fpki-common-High shall contain RSA public keys that are 2048 or 3072 bits or elliptic curve keys that are 256 or 384 bits.~~

Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP ~~shall~~must require (1) ~~triple-DES or~~ AES for the symmetric key ~~through December 31, 2010 and AES for the symmetric key after December 31, 2010 and~~ and (2) at least ~~1024~~ 2048-bit RSA or ~~163~~ 256-bit elliptic curve keys ~~through December 31, 2008,~~ , and at least ~~2048 bit RSA or 224 bit elliptic curve keys after December 31, 2008, and~~ 3072-bit RSA or at least 256-bit elliptic curve keys after December 31, 2030.

6.1.6. Public Key Parameters Generation and Quality Checking

Elliptic curve public key parameters ~~shall~~must always be selected from the set specified in Section 7.1.3.

6.1.7. Key Usage Purposes (as per X.509 v3 Key Usage Field)

The use of a specific key is constrained by the Key Usage extension in the X.509 certificate. ~~All certificates shall include a critical key usage extension.~~

~~Public keys that are bound into subscriber user~~All certificates ~~shall~~must include a critical Key Usage extension.

The dataEncipherment, encipherOnly, and decipherOnly bits must not be asserted in certificates issued under this policy.

- Certificates to be used for authentication must set only ~~for signing~~the digitalSignature bit.
- Certificates to be used by Human Subscribers only for digital signatures must set the digitalSignature and nonRepudiation bits.
- Certificates that have the nonRepudiation bit set, must not have keyEncipherment bit or ~~encrypting~~keyAgreement bit set.
- Certificates to be used for encryption (RSA) must set the keyEncipherment bit.
- Certificates to be used for key agreement (ECC) must set the keyAgreement bit.
- CA certificates must set only cRLSign and keyCertSign bits.

Keys associated with CA certificates must be used only for signing certificates and CRLs.

Keys associated with Human Subscriber certificates must be used only for digital signature (including authentication) or encryption, but not both.

~~User~~ Certificates that assert id-fpki-common-authentication, id-fpki-common-pivi-authentication, id-fpki-common-derived-pivAuth- hardware, id-fpki-common-derived-pivAuth, id-fpki-common-cardAuth, or id-fpki-common-pivi-cardAuth ~~shall only assert the *digitalSignature* bit. Other user certificates to be used for digital signatures shall assert both the *digitalSignature* and *nonRepudiation* bits. User certificates that contain RSA public keys that are to be used for key transport shall assert the *keyEncipherment* bit. User certificates that contain elliptic curve public keys that are to be used for key agreement shall assert the *keyAgreement* bit~~are used solely for authentication.

~~Public keys that are bound into CA certificates shall be used only for signing certificates and status information (e.g., CRLs). CA certificates whose subject public key is to be used to verify other certificates shall assert the *keyCertSign* bit. CA certificates whose subject public key is to be used to verify CRLs shall assert the *cRLSign* bit. CA certificates whose subject public key is to be used to verify Online Certificate Status Protocol (OCSP) responses shall assert the *digitalSignature* and/or *nonRepudiation* bits.~~

~~Public keys that are bound into device~~Keys associated with Device Subscriber certificates may be used for digital signature (including authentication), ~~key management~~encryption, or both. ~~Device certificates to be used for digital signatures shall assert the *digitalSignature* bit.~~ Device certificates ~~that contain RSA public keys that are to be used for key transport shall assert the *keyEncipherment* bit. Device certificates that contain elliptic curve public keys that are to be used for key agreement shall assert the *keyAgreement* bit. Device certificates to be used for both digital signatures and key management shall assert the *digitalSignature* bit and either the *keyEncipherment* (for RSA) or *keyAgreement* (for elliptic curve) bit. Device certificates shall~~must not assert the nonRepudiation bit.

~~The *dataEncipherment*, *encipherOnly*, and *decipherOnly* bits shall not be asserted in certificates issued under this policy.~~

For ~~End Entity~~all Subscriber certificates issued after June 30, 2019, the Extended Key Usage extension ~~shall~~must always be present~~ and shall not contain *anyExtendedKeyUsage* {2.5.29.37.0}.~~.

For all Subscriber certificates, Extended Key Usage OIDs ~~shall~~must be consistent with key usage bits asserted. The Extended Key Usage extension must not contain anyExtendedKeyUsage {2.5.29.37.0} or id-kpcodeSigning {1.3.6.1.5.5.7.3.3}.

~~If a certificate is used for authentication of ephemeral keys, the Key Usage bit in the certificate must assert the *digitalSignature* bit and may or may not assert *keyEncryption* and *keyAgreement* depending on the public key in the SPKI of the certificate.~~

~~Signing certificates issued under the policy for~~ Certificates that assert id-fpki-common-piv-contentSigning ~~or~~ must include a critical Extended Key Usage extension that asserts only id-PIV-content-signing {2.16.840.1.101.3.6.7} (see [CCP-PROF]).

Certificates that assert id-fpki-common-pivi-contentSigning ~~shall~~must include ~~an extended key usage of~~a critical Extended Key Usage extension that asserts only id-~~*PIV*~~fpki-pivi-content-signing {2.16.840.1.101.3.8.7} (see [~~CCP-PROF~~PIV-I Profile]).

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is Security Requirements for Cryptographic Modules [FIPS 140~~-2].~~]. A FIPS 140 Level 1 or higher validated cryptographic module must be used for all cryptographic operations. Cryptographic modules ~~shall~~must be minimally validated to a FIPS 140 level identified in this section.

~~In accordance with FIPS 201, the relevant NIST Guideline for PIV Card Issuers (PCI) and Derived PIV Credential Issuers is NIST SP 800-79, *Guidelines for the Accreditation of PCIs and Derived PIV Credential Issuers* (DPCI), which utilizes various aspects of NIST SP 800-37 and applies them to accrediting the reliability of PCIs and DPCIs.~~

~~CAs that issue certificates under id-fpki-common-High shall use a FIPS 140 Level 3 or higher validated hardware cryptographic module. CAs that do not issue certificates under id-fpki-common-High shall~~

Private Key	FIPS 140 Level
CA ● all applicable policies	3
CSS ● all applicable policies	2
PIV and Common PIV-I Content Signing ● id-fpki-common-piv-contentSigning ● id-fpki-common-pivi-contentSigning	2
Hardware Signature and Authentication ● id-fpki-common-authentication ● id-fpki-common-derived-pivAuth-hardware ● id-fpki-common-cardAuth ● id-fpki-common-hardware ● id-fpki-common-high ● id-fpki-common-pivi-authentication ● id-fpki-common-pivi-cardAuth	2
Hardware Subscriber Key Management ● id-fpki-common-hardware	2
Hardware Device ● id-fpki-common-devicesHardware	2
Software Signature and Authentication ● id-fpki-common-policy ● id-fpki-common-derived-pivAuth	1
Software Subscriber Key Management ● id-fpki-common-policy	1
Software Device ● id-fpki-common-devices	1

RAs must use a FIPS 140 Level 2 or higher validated hardware cryptographic module when authenticating to systems to fulfill their duties.

~~RAs shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module.~~

~~PIV Cards are PKI tokens that have private keys associated with certificates asserting id-fpki-common-authentication or id-fpki-common-cardAuth. PIV Cards shall~~PIV or Common PIV-I cards must only be issued using card stock that has been tested and approved by the FIPS 201 Evaluation Program and listed on the GSA ~~Approved Products List (APL).~~

~~PIV-I cards have private keys associated with certificates asserting id-fpki-common-pivi-authentication or id-fpki-common-pivi-cardAuth. PIV-I cards issued by federal executive branch agencies and the certification authorities operating under this policy shall only be issued using card stock that has been tested and approved by the FIPS 201 Evaluation Program and listed on the GSA~~ Approved Products List (APL). Card stock that has been removed from the APL may continue to be issued for no more than one year after GSA approved replacement card stock is available. ~~Smart~~PIV or Common PIV-I cards issued using the deprecated card stock may continue to be used until the current Subscriber certificates expire, unless otherwise notified by the FPKIPA/FPKIMA. ~~On an annual basis, for each PCI configuration used (as defined by the FIPS 201 Evaluation Program), one populated, representative sample PIV and/or PIV-I Card shall be submitted to the FIPS 201 Evaluation Program for testing.~~

~~Subscribers shall use a FIPS 140 Level 1 or higher validated cryptographic module for all cryptographic operations. Subscribers issued certificates under the hardware users policy (id-fpki-common-hardware or id-fpki-common-devicesHardware), one of the authentication policies (id-fpki-common-authentication, id-fpki-common-pivi-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-cardAuth, or id-fpki-common-pivi-cardAuth), or common High policy (id-fpki-common-High) shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module for all private key operations.~~

~~CSSes that provide status information for certificates issued under id-fpki-common-High shall use a FIPS 140 Level 3 or higher validated hardware cryptographic module. CSSes that do not provide status information for certificates issued under id-fpki-common-High shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module.~~

Any pseudo-random numbers used for key generation material must be generated using a FIPS-validated cryptographic module.

6.2.2. Private Key (n out of m) Multi-Person Control

A single person ~~shall~~must not be permitted to activate or access any cryptographic module that contains the complete CA private signing key. CA signature keys may be backed up only under two-person control. Access to CA signing keys backed up for disaster recovery ~~shall~~must be under at least two-person control. The names of the parties used for two-person control ~~shall~~must be maintained on a list that ~~shall~~must be made available for inspection during compliance audits.

6.2.3. Private Key Escrow

CA private keys are never escrowed.

Human Subscriber key management keys ~~shall~~must be escrowed to provide key recovery as described in Section 4.12.1. If a device has a separate key management key certificate, the key management private key may be escrowed.

6.2.4. Private Key Backup

~~6.2.4.1. Backup~~All backups of the CA~~ Private Signature Key~~

~~The CA~~, CSS and PIV Content Signing private signature keys ~~shall~~must be ~~backed up~~accounted for and protected under the same ~~multiperson~~multi-person control as the original signature key. At least one copy of the ~~private signature key shall be stored off-site. All copies of the~~ CA private signature key ~~shall be accounted for and protected in the same manner as the original. Backup procedures shall be included in the CA's CPS~~must be stored off-site. For all other keys, backup, when permitted, must provide security controls consistent with the protection provided by the original cryptographic module. Backed up private signature key(s) must not be exported or stored in plaintext form outside the cryptographic module.

~~6.2.4.2. Backup of Subscriber Private Signature Key~~

~~Subscriber private signature keys whose corresponding public key is contained in a certificate asserting the id-fpki-common-authentication, id-fpki-common-pivi-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-cardAuth, id-fpki-common-pivi-cardAuth, or id-fpki-common-High policy shall not be backed up or copied.~~

~~All other~~

Private Key	Backup
CA ● all applicable policies	Required
CSS ● all applicable policies	Optional
PIV and Common PIV-I Content Signing ● id-fpki-common-piv-contentSigning ● id-fpki-common-pivi-contentSigning	Optional
Hardware Signature and Authentication ● id-fpki-common-authentication ● id-fpki-common-derived-pivAuth-hardware ● id-fpki-common-cardAuth ● id-fpki-common-hardware ● id-fpki-common-high ● id-fpki-common-pivi-authentication ● id-fpki-common-pivi-cardAuth	Not Permitted
Hardware Subscriber Key Management ● id-fpki-common-hardware	Required
Hardware Device ● id-fpki-common-devicesHardware	Optional
Software Signature and Authentication	Optional *

• id-fpki-common-policy • id-fpki-common-derived-pivAuth	
Software Subscriber Key Management • id-fpki-common-policy	Required
Software Device • id-fpki-common-devices	Optional

* Software Subscriber private signature keys may be backed up or copied, but must be held in the Subscriber's control. ~~Backed up subscriber private signature keys shall not be stored in plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.~~

~~6.2.4.3. Backup of Subscriber Private Key Management Key~~

~~Backed up subscriber private key management keys shall not be stored in plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.~~

~~6.2.4.4. Backup of CSS Private Key~~

~~CSS private keys may be backed up. If backed up, all copies shall be accounted for and protected in the same manner as the original.~~

~~6.2.4.5. Backup of Device Private Keys~~

~~Device private keys may be backed up or copied, but must be held under the control of the device's human sponsor or other authorized administrator. Backed up device private keys shall not be stored in plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the device's cryptographic module.~~

~~6.2.4.6. Backup of Common PIV Content Signing Key~~

~~The Common PIV Content Signing private signature keys shall be backed up under multi-person control. At least one copy of the private signature key shall be stored in a secondary location. All copies of the Common PIV Content Signing private signature key shall be accounted for and protected in the same manner as the original. Backed up Common PIV Content private signature keys shall not be exported or stored in plaintext form outside the cryptographic module. Backup procedures shall be documented.~~

6.2.5. Private Key Archival

CA private signature keys and Subscriber private ~~signatures~~signature keys ~~shall~~must not be archived. CAs that retain Subscriber private encryption keys for business continuity purposes ~~shall~~must archive such Subscriber private keys, in accordance with Section 5.5.

6.2.6. Private Key Transfer into or from a Cryptographic Module

~~CA private~~At no time shall the CA private key exist in plaintext outside the cryptographic module boundary.

CA, CSS and PIV Content Signing private signature keys may be exported from the cryptographic module only to perform ~~CA~~ key backup procedures as described in Section 6.2.4.~~1. At no time shall the CA private key exist in plaintext outside the cryptographic module.~~

~~All other keys shall be generated by and in a cryptographic module.~~ In the event that ~~a~~any private key is ~~to be~~ transported from one cryptographic module to another, the private key must be ~~encrypted during transport;~~protected using a FIPS approved algorithm and at a bit strength commensurate with the key being transported. Private keys must never exist in plaintext form outside the cryptographic module boundary.

Private or symmetric keys used to encrypt other private keys for transport must be protected from disclosure.

6.2.7. Private Key Storage on Cryptographic Module

No stipulation beyond that specified in [FIPS 140~~.~~].

6.2.8. Method of Activating Private Key

~~For certificates issued under id-fpki-common-authentication, id-fpki-common-pivi-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-derived-pivAuth, id-fpki-common-policy, id-fpki-common-hardware, and id-fpki-common-High, the subscriber must be authenticated to the cryptographic token before the activation of the associated private key(s). Acceptable means of authentication include but are not limited to passphrases, PINs or biometrics. When passphrases or PINs are used, they shall be a minimum of six (6) characters. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).~~

~~For certificates issued under id-fpki-common-devices and id-fpki-common-devicesHardware, the device may be configured to activate its private key without requiring its human sponsor or authorized administrator to authenticate to the cryptographic token, provided that appropriate physical and logical access controls are implemented for the device and its cryptographic token. For certificates issued under id-fpki-common-piv-contentSigning or id-fpki-common-pivi-contentSigning, the PIV card issuance system or device may be configured to activate its private key without requiring its human sponsor or authorized administrator to authenticate to the cryptographic token, provided that appropriate physical and logical access controls are implemented for content signing operations conformant with PIV issuance requirements (see [FIPS 201]). The strength of the security controls shall be commensurate with the level of threat in the device's environment, and shall protect the device's hardware, software, and the cryptographic token and its activation data from compromise.~~

~~For certificates issued under id-fpki-common-cardAuth or id-fpki-common-pivi-cardAuth, subscriber authentication is not required to use the associated private key.~~

Cryptographic modules must be protected from unauthorized access.

Subscriber private key activation requirements are detailed in the following table:

Policy Asserted	Activation Requirements
id-fpki-common-authentication id-fpki-common-derived-pivAuth-hardware id-fpki-common-derived-pivAuth id-fpki-common-policy id-fpki-common-hardware id-fpki-common-high id-fpki-common-pivi-authentication	Passphrases, PINs or biometrics. When passphrases or PINs are used, they must be a minimum of six (6) characters. Entry of activation data must be protected from disclosure (i.e., the data should not be displayed while it is entered).
id-fpki-common-devices and id-fpki-common-devicesHardware	May be configured to activate the private key without requiring a human sponsor or authorized administrator to authenticate to the cryptographic token. The appropriate physical and logical access controls must be implemented for the device and its cryptographic token.
id-fpki-common-piv-contentSigning id-fpki-common-pivi-contentSigning	May be configured to activate the private key without requiring a human sponsor or authorized administrator to authenticate to the cryptographic token. The appropriate physical and logical access controls must be implemented for content signing operations conformant with PIV issuance requirements (see [FIPS 201]). The strength of the security controls must be commensurate with the level of threat in the PIV credential issuance system's environment, and must protect the hardware, software, and the cryptographic token and its activation data from compromise.
id-fpki-common-cardAuth id-fpki-common-pivi-cardAuth	None.

6.2.9. Method of Deactivating Private Key

~~Cryptographic modules that have been activated shall not be available to unauthorized access.~~ After use, the cryptographic module ~~shall~~must be deactivated~~, e.g.,~~ via a manual logout procedure or automatically after a period of inactivity as defined in the applicable CPS. CA cryptographic modules ~~shall~~must be ~~removed and stored~~physically secured per requirements in ~~a secure container~~Section 5.1 when not in use.

6.2.10. Method of Destroying Private Key

Individuals in Trusted Roles ~~shall~~must destroy all copies of CA, RA, and CSS (e.g., OCSP server) private signature keys and activation data (e.g. operator card set or tokens) when they are no longer needed. Subscribers ~~shall~~must either surrender their cryptographic module to CA/RA personnel for destruction or destroy their private signature keys, when they are no longer needed or when the certificates to which they correspond expire or are revoked. Physical destruction of hardware is not required.

~~Practice Note: Destruction will likely be performed by executing a “zeroize” command.~~

Practice Note: Destruction will likely be performed by executing a “zeroize” command.

To ensure future access to encrypted data, Subscriber private key management keys should be secured in long-term backups or archived.

6.2.11. Cryptographic Module Rating

See Section 6.2.1.

6.3. *Other Aspects of Key Pair Management*

6.3.1. Public Key Archival

The public key is archived as part of the certificate archival.

6.3.2. Certificate Operational Periods and Key Usage Periods

~~The usage period for~~For CAs such as the Federal Common Policy ~~Root CA key pair~~ CA that issue certificates only to other CAs or CSSs, the maximum key usage period is ~~a maximum of~~ 20 years.

~~For all other~~All CAs operating under this policy that issue Subscriber certificates, the usage period for a CA key pair is a maximum of ~~ten~~10 years.~~ The~~[4]

[4] Content Signing and OCSP Signing certificates are excluded from this requirement.

A CA private key ~~may be used to sign certificates for at most four years, but~~ may be used to sign CRLs and OCSP responder certificates for the entire usage period. All certificates signed by a specific CA key pair must expire before the end of that key pair's usage period.

~~Subscriber public keys in certificates that assert the id-PIV-content-signing or id-fpki-common-pivi-contentSigning OID in the extended key usage extension have a maximum usage period of nine years. The private keys corresponding to the public keys in these certificates have a maximum usage period of three years. Expiration of the id-fpki-common-piv-contentSigning or id-fpki-common-pivi-contentSigning certificate shall be later than the expiration of the credential's id-fpki-common-authentication, id-fpki-common-pivi-authentication, id-fpki-common-derived-pivAuth-hardware, or id-fpki-common-derived-pivAuth certificates.~~

~~For OCSP responders operating under this policy and all other subscriber public keys, the maximum usage period is three years. Subscriber signature private keys have the same usage period as their corresponding public key. The usage period for subscriber key management private keys is not restricted.~~

Key	Private Key	Certificate
Subscriber Authentication	3 years	3 years
Subscriber Signature	3 years	3 years
Subscriber Encryption	Unrestricted	3 years
Card Authentication	3 years	3 years
Content Signing	3 Years	9 Years *
OCSP Responder	3 years	120 days
Device	3 years	3 years

* Expiration of the Content Signing certificate must be later than the expiration of the Subscriber certificates on the same PIV credential.

6.4. ACTIVATION DATA

6.4.1. Activation Data Generation and Installation

CA activation data may be user-selected (by each of the multiple parties holding that activation data). If the activation data must be transmitted, it ~~shall~~must be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

RA and Subscriber activation data may be user-selected. The strength of the activation data ~~shall~~must meet or exceed the requirements for authentication mechanisms stipulated for Level 2 in [FIPS 140~~-2.~~]. If the activation data must be transmitted, it ~~shall~~must be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

6.4.2. Activation Data Protection

Data used to unlock private keys ~~shall~~must be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data ~~shall~~must be:

- memorized;
- biometric in nature; or
- recorded and secured at the level of assurance associated with the activation of the cryptographic module, and ~~shall~~must not be stored with the cryptographic module.

~~Practice Note: Level 2 in FIPS 140-2 requires that the protection mechanism includes a facility to protect against repeated guessing attacks.~~

Practice Note: Level 2 in [FIPS 140] requires that the protection mechanism includes a facility to protect against repeated guessing attacks.

6.4.3. Other Aspects of Activation Data

~~No stipulation.~~

A CA operating under this policy must define any other aspects of Activation Data in its CPS.

6.5. COMPUTER SECURITY CONTROLS

6.5.1. Specific Computer Security Technical Requirements

~~Computer security controls are required to ensure CA/RA operations are performed as specified in~~For CAs operating under this policy~~. The following~~ , the computer security functions ~~pertaining to the Common Policy Root CA~~listed below are required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards~~:~~

- ~~Require authenticated logins~~

- ~~Provide discretionary access control~~
- ~~Provide a security audit capability~~
- ~~Enforce access control for CA services and PKI roles~~
- ~~Enforce separation of duties for PKI roles~~
- ~~Require identification and authentication of PKI roles and associated identities~~
- ~~Prohibit object reuse or require separation for CA random access memory~~
- ~~Require use of cryptography for session communication and database security~~
- ~~Archive CA history and audit data~~
- ~~Require self-test security-related CA services~~
- ~~Require a trusted path for identification of PKI roles and associated identities~~
- ~~Require a recovery mechanism for keys and the CA system~~
- ~~Enforce domain integrity boundaries for security-critical processes.~~

~~For those portions of the Common Policy Root CA operating in a VME, the following security functions also pertain to the hypervisor:~~

- ~~Require authenticated logins~~
- ~~Provide discretionary access control~~
- ~~Provide a security audit capability~~
- ~~Enforce separation of duties for PKI roles~~
- ~~Prohibit object reuse or require separation for CA random access memory~~
- ~~Require use of cryptography for session communication and database security~~
- ~~Archive CA history and audit data~~
- ~~Require self-test security-related CA services~~
- ~~Enforce domain integrity boundaries for security-critical processes.~~

~~For other CAs operating under this policy, the computer security functions listed below are required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards.~~. The CA and its ancillary parts ~~shall~~must include the following functionality (in a VME, these functions are applicable to both the VM and hypervisor):

- authenticate the identity of users before permitting access to the system, data, or applications;
- manage privileges of users to limit users to their assigned roles;
- generate and archive audit records for all transactions; (see Section 5.4)
- enforce domain integrity boundaries for security critical processes; ~~and~~
- ~~support~~require use of cryptography for session communication and database security;

- require self-test security-related CA services;
- require a trusted path for identification of all users;
- provide residual information protection; and
- require recovery from key or system failure.

For certificate status servers operating under this policy, the computer security functions listed below are required (in a VME, these functions are applicable to both the VM and hypervisor):

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- enforce domain integrity boundaries for security critical processes; ~~and~~
- ~~support~~provide residual information protection; and
- require recovery from key or system failure.

For remote workstations used to administer the CAs, the computer security functions listed below are required:

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- generate and archive audit records for all transactions; (see Section 5.4)
- enforce domain integrity boundaries for security critical processes; ~~and~~
- ~~support~~provide residual information protection; and
- require recovery from ~~key or~~ system failure.

All communications between any PKI Trusted Role and the CA ~~shall~~must be authenticated and protected from modification.

6.5.2. Computer Security Rating

~~No Stipulation.~~

CAs operating under this policy must identify any Computer Security Rating requirements in the applicable CPS.

6.6. LIFE CYCLE TECHNICAL CONTROLS

6.6.1. System Development Controls

The system development controls for the CA (including any remote workstations used to administer the CA) and RA are as follows:

- ~~The CA shall use software that has been designed and developed under a formal, documented development methodology.~~
- Hardware and software ~~procured~~used to administer or operate the CA ~~shall~~must be ~~purchased~~procured in a fashion to reduce the likelihood that any particular component was

tampered with (e.g., by ensuring the vendor cannot identify the PKI component that will be installed on a particular device).

- Custom hardware and software ~~developed specifically for the CA shall~~must be developed in a controlled environment, and the development process ~~shall~~must be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.
- The CA hardware and software, including the VME hypervisor, ~~shall~~must be dedicated to operating and supporting the CA (i.e., the systems and services dedicated to the issuance and management of certificates). There ~~shall~~must be no other applications, hardware devices, network connections, or component software installed that are not parts of the CA operation~~.~~, administration, monitoring and security compliance of the system. Where the CA operation supports multiple CAs, the hardware platform may support multiple CAs. In a VME, a single hypervisor may support multiple CAs and their supporting systems, provided all systems have comparable security controls and are dedicated to the support of the CA.
- ~~In~~If a ~~VME~~CA operates in a VM, all VM systems in that VMS must operate in the same security zone as the CA.
- Proper care ~~shall~~must be taken to prevent malicious software from being loaded onto the CA equipment. All applications required to perform the operation of the CA ~~shall~~must be obtained from documented sources. With the exception of Offline CAs, CA and RA hardware and software ~~shall~~must be scanned for malicious code on first use and periodically thereafter.
- Hardware and software updates ~~shall~~must be purchased or developed in the same manner as original equipment, and ~~shall~~must be installed by trusted and trained personnel in a defined manner.

6.6.2. Security Management Controls

The configuration of the CA system, in addition to any modifications and upgrades, ~~shall~~must be documented and controlled. There ~~shall~~must be a mechanism for detecting unauthorized modification to the software or configuration. The CA software, when first loaded, ~~shall~~must be verified as being that supplied from the vendor, with no modifications, and be the version intended for use. The CA ~~shall~~must periodically verify the integrity of the software~~ as specified in the CPS~~.

6.6.3. Life Cycle Security Controls

~~No stipulation.~~

CAs operating under this policy must identify any Life Cycle Security Control requirements in the applicable CPS.

6.7. NETWORK SECURITY CONTROLS

This section does not apply to offline CAs.

A network guard, firewall, or filtering router must protect network access to CA equipment. The network guard, firewall, or filtering router ~~shall~~must limit services allowed to and from the CA equipment to those required to perform CA functions.

Protection of CA equipment ~~shall~~must be provided against known network attacks. All unused network ports and services ~~shall~~must be turned off. Any network software present on the CA equipment ~~shall~~must be necessary to the functioning of the CA application.

Any boundary control devices used to protect the network on which PKI equipment is hosted ~~shall~~must deny all but the necessary services to the PKI equipment.

Repositories, ~~certificate status servers~~CSSs, and remote workstations used to administer the CAs ~~shall~~must employ appropriate network security controls. Networking equipment ~~shall~~must turn off unused network ports and services. Any network software present ~~shall~~must be necessary to the ~~functioning~~function of the equipment.

~~The CA shall establish connection with a~~The remote workstation used to administer the CA ~~only after successful~~ must use a VPN to access the CA. The VPN must be configured for mutual authentication, encryption and integrity. If mutual authentication is shared secret based, the shared secret must be changed at least annually, must be randomly generated, and must have entropy commensurate with the cryptographic strength of ~~the~~certificates issued by the PKI being administered.

The CA must permit remote ~~workstation~~administration only after successful multi-factor authentication of the Trusted Role at a level of assurance commensurate with that of the CA.

6.8. TIME-STAMPING

Asserted times ~~shall~~must be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events (see Section 5.4.1).

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. CERTIFICATE PROFILE

Certificates issued by a CA under this policy ~~shall~~must conform to the Common Policy X.509 Certificate and Certificate Revocation List (CRL) ~~Extensions Profile for the Shared Service Providers (SSP) Program~~Profiles [CCP-PROF].

7.1.1. Version Number(s)

~~The CA shall issue~~Certificates must be of type X.509 v3~~ certificates~~ (populate version field with integer “2”).

7.1.2. Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in [CCP~~-~~-PROF].

7.1.3. Algorithm Object Identifiers

Certificates ~~issued under this CP shall~~must use the following OIDs for signatures:

Signature Algorithm	Object Identifier
sha256WithRSAEncryption ~~sha-1WithRSAEncryption~~	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs~~-~~-1(1) ~~5}~~11} (1.2.840.113549.1.1.11)
sha384WithRSAEncryption ~~sha256WithRSAEncryption~~	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs~~-~~-1(1) ~~11}~~12} (1.2.840.113549.1.1.12)
~~RSA with PSS padding~~sha512WithRSAEncryption	~~id-RSASSA-PSS ::= ~~{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) ~~10}~~13} (1.2.840.113549.1.1.13)
id-RSASSA-PSS	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10} (1.2.840.113549.1.1.10)
ecdsa-with-SHA256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2} (1.2.840.10045.4.3.2)
ecdsa-with-SHA384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3} (1.2.840.10045.4.3.3)
ecdsa-with-SHA512	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) 4} (1.2.840.10045.4.3.4)

The PSS padding scheme OID is independent of the hash algorithm~~;~~. The hash algorithm is specified as a parameter (for details, see [PKCS#1]). Certificates issued under this CP must use the SHA-256 hash algorithm when generating RSASSA-PSS signatures. The following OID ~~shall~~must be used to specify the hash in an RSASSA-PSS digital signature:

SHA-256	~~id-sha256 ::= ~~{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1} (2.16.840.1.101.3.4.2.1)

Certificates ~~issued under this CP shall~~must use the following OIDs to identify the algorithm associated with the subject key:

Public Key Algorithm	Object Identifier
rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1} (1.2.840.113549.1.1.1)
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1} (1.2.840.10045.2.1)

Where the certificate contains an elliptic curve public key, the parameters ~~shall~~must be specified as one of the following named curves:

Curve	Object Identifier
ansip256r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7} (1.2.840.10045.3.1.7)
ansip384r1	{iso(1) identified-organization(3) certicom(132) curve(0) 34 } (1.3.132.0.34)

7.1.4. Name Forms

The subject ~~field in~~and issuer fields of certificates issued under ~~id-fpki-common-~~this policy~~, id-fpki-common-hardware, id-fpki-common-authentication, id-fpki-common-pivi-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-derived-pivAuth, id-fpki-common-High, id-fpki-common-devices, id-fpki-common-devicesHardware, id-fpki-common-piv-contentSigning, and id-fpki-common-pivi-contentSigning shall~~ must be populated with an X.500 Distinguished Name as specified in Section 3.1.1.

~~The issuer field of certificates issued under the policies in this document shall be populated with a non-empty X.500 Distinguished Name as specified in section 3.1.1.~~

~~The subject alternative name extension shall be present and include the pivFASC-N name type in certificates issued under id-fpki-common-authentication and id-fpki-common-cardAuth.~~

~~The subject alternative name extension shall be present and include a UUID, encoded as a URI, in certificates issued under id-fpki-common-authentication, id-fpki-common-cardAuth, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-derived-pivAuth, id-fpki-common-pivi-authentication, and id-fpki-common-pivi-cardAuth.~~

7.1.5. Name Constraints

~~The CAs may assert~~ Name constraints may be asserted in CA certificates.

7.1.6. Certificate Policy Object Identifier

Certificates issued under this CP ~~shall~~must assert at least one ~~of the following OIDs~~policy OID as specified in Section 1.2 in the certificate policies extension~~, as appropriate:~~.

~~id-fpki-common-policy ::= {2 16 840 1 101 3 2 1 3 6}~~

~~id-fpki-common-hardware ::= {2 16 840 1 101 3 2 1 3 7}~~

~~id-fpki-common-devices ::= {2 16 840 1 101 3 2 1 3 8}~~

~~id-fpki-common-devicesHardware ::= {2 16 840 1 101 3 2 1 3 36}~~

~~id-fpki-common-authentication ::= {2 16 840 1 101 3 2 1 3 13}~~

~~id-fpki-common-derived-pivAuth ::= {2 16 840 1 101 3 2 1 3 40}~~

~~id-fpki-common-derived-pivAuth-hardware ::= {2 16 840 1 101 3 2 1 3 41}~~

~~id-fpki-common-High ::= {2 16 840 1 101 3 2 1 3 16}~~

~~id-fpki-common-cardAuth ::= {2 16 840 1 101 3 2 1 3 17}~~

~~id-fpki-common-piv-contentSigning ::= {2 16 840 1 101 3 2 1 3 39}~~

~~id-fpki-common-pivi-authentication ::= {2 16 840 1 101 3 2 1 3 45}~~

~~id-fpki-common-pivi-cardAuth ::= {2 16 840 1 101 3 2 1 3 46}~~

~~id-fpki-common-pivi-contentSigning ::= {2 16 840 1 101 3 2 1 3 47}~~

Certificates that express the id-fpki-common-cardAuth, id-fpki-common-pivi-cardAuth, id-fpki-common-piv-contentSigning, or id-fpki-common-pivi-contentSigning policy OID ~~shall~~must not express any other policy OIDs.

Delegated OCSP Responder certificates must assert all policy OIDs for which they are authoritative.

7.1.7. Usage of Policy Constraints Extension

The CAs may assert policy constraints in CA certificates. When this extension appears, at least one of requireExplicitPolicy or inhibitPolicyMapping must be present. ~~When present, this extension should be marked as noncritical*, to support legacy applications that cannot process *policyConstraints*. For Subordinate CA certificates *inhibitPolicyMappings*, skip certs will be set to 0. For cross-certificates *inhibitPolicyMappings*, skip certs will be set to 1, or 2 for the Federal Bridge CA. When *requireExplicitPolicy* is included, skip certs will be set to 0~~ When present, this extension may be marked critical.

For certificates issued to the Federal Bridge CA, inhibitPolicyMappings skip certs must be set to 2.

For all other CA certificates issued by the Federal Common Policy CA, inhibitPolicyMappingskip certs must be set to 0. When requireExplicitPolicy is included, skip certs must be set to 0.

7.1.8. Policy Qualifiers Syntax and Semantics

Certificates issued under this CP ~~shall not~~may contain a policy ~~qualifiers~~qualifier containing a CPS URI.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

Certificates issued under this policy ~~shall not~~must contain a non-critical certificate policies extension.

7.1.10. Inhibit Any Policy Extension

The CAs may assert InhibitAnyPolicy in CA certificates. When present, this extension ~~should~~may be marked ~~as noncritical*, to support legacy applications that cannot process *InhibitAnyPolicy*.~~critical. Skip certs ~~shall~~must be set to 0, since certificate policies are required in the Federal PKI.

~~*Note: The recommended criticality setting is different from RFC 5280.~~

7.2. CRL Profile

CRLs issued by a CA under this CP ~~shall~~must conform to the CRL profile specified in [CCP-PROF].

7.2.1. Version Number(s)

The CAs ~~shall~~must issue X.509 Version two (2) CRLs.

7.2.2. CRL and CRL Entry Extensions

Detailed CRL profiles addressing the use of each extension are specified in [CCP-PROF].

7.3. OCSP Profile

~~Certificate status servers (~~CSSs~~)~~ operated under this policy ~~shall~~must sign responses using algorithms designated for CRL signing.

All CSSs ~~shall be able to process~~must accept and return SHA-1 hashes ~~when included~~ in the CertID ~~field~~ and ~~the keyHash in the~~ responderID ~~field~~fields. CSS may accept and return additional hash algorithms within the CertID fields. CSSs must not return any response containing a hash algorithm in the CertID that differs from the CertID in the request.

7.3.1. Version Number(s)

CSSs operated under this policy ~~shall~~must use OCSP version 1.

7.3.2. OCSP Extensions

Critical OCSP extensions ~~shall~~must not be used.

8. Compliance Audit and Other Assessments

CAs operating under this policy are subject to an annual review by the FPKIPA to ensure their policies and operations remain compliant with this policy.

CAs operating under this policy ~~shall~~must have a compliance audit mechanism in place to ensure that the requirements of their CPS are being implemented and enforced. The ~~SSP~~organization's PMA ~~shall~~must be responsible for ensuring annual audits are conducted for all PKI functions regardless of how or by whom the PKI components are managed and operated.

Agencies must ensure they have appropriate authority to operate, in accordance with [FIPS 201] and [NIST SP 800-79] Guidelines for the Accreditation of PIV Card Issuers and Derived PIV Credential Issuers (DPCI). Agencies must also ensure annual PKI compliance audits are conducted for all PKI operations for which they are responsible.

For the Federal Common Policy ~~Root~~ CA, the FPKIMA ~~shall~~must have a compliance audit mechanism in place to ensure that the requirements of this CP are being implemented and enforced by its CPS.

This CP does not impose a requirement for any particular assessment methodology.

8.1. Frequency or Circumstances of Assessment

~~This specification does not impose a requirement for any particular assessment methodology.~~

~~8.1.1.1. Frequency or Circumstances of Assessment~~

CAs and RAs operating under this policy ~~shall~~must be subject to ~~a periodic~~an annual compliance audit ~~at least once per year~~ in accordance with the FPKI Annual Review Requirements document [AUDIT]. The FPKIPA has the right to require aperiodic compliance audits of CAs operating under this policy.

~~Further, The FPKIPA has the right to require aperiodic compliance audits of CAs operating under this policy.~~ The FPKIPA ~~shall~~must state the reason for any aperiodic compliance audit.

On an annual basis, for each PCI configuration used (as defined by the FIPS 201 Evaluation Program), one populated, representative PIV credential must be submitted to the FIPS 201 Evaluation Program for testing.

8.2. Identity/Qualifications of Assessor

The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the CA's CPS and this CP. The compliance auditor must perform such compliance audits as a regular ongoing business activity. In addition to the previous requirements, the auditor must be a certified information system auditor (CISA) or IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The compliance auditor either ~~shall~~must be a private firm that is independent from the entities (CA and RAs) being audited, or it ~~shall~~must be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. An example of the latter situation may be an agency inspector general. To ~~insure~~ensure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining the entity's CA facility or ~~certificate practices statement.~~Certification Practices Statement. The FPKIPA ~~shall~~may determine whether a compliance auditor meets this requirement.

~~The Agency PMA~~Each agency is responsible for identifying and engaging a qualified auditor of agency operations implementing aspects of this CP.

8.4. TOPICS COVERED BY ASSESSMENT

The purpose of a compliance audit ~~shall~~must be to verify that a CA ~~operated by a SSP~~ and ~~all~~its RAs ~~of that CA~~ comply with all the requirements of the current versions of ~~the Federal Common Policy Root CA~~this CP and the ~~SSP's~~CA's CPS. All aspects of the CA/RA operation ~~shall~~must be subject to compliance audit inspections. Components other than CAs may be audited fully or by using a representative sample. ~~If the auditor uses statistical sampling, all PKI components, PKI component managers and operators shall be considered in the sample. The samples shall vary on an annual basis.~~

If the compliance auditor uses statistical sampling, all PKI components, PKI component managers and operators must be considered in the sample. The samples must vary on an annual basis.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

When the compliance auditor or FIPS 201 Evaluation Program testing finds a discrepancy between the requirements of this CP or the stipulations in the CPS and the design, operation, or maintenance of the PKI Authorities, the following actions ~~shall~~must be performed:

- ~~The compliance auditor shall note~~ The discrepancy must be documented;
- ~~The compliance auditor shall notify~~ The responsible party ~~promptly~~must be notified; and
- The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to the FPKIPA and appropriate agency ~~PMA~~.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the FPKIPA may decide to temporarily halt operation of the CA or RA, to revoke a certificate issued to the CA or RA, or take other actions it deems appropriate. The FPKIPA will develop procedures for making and implementing such determinations. ~~In accordance with section 8.1,~~ A compliance audit or FIPS 201 Evaluation Program test may be required to confirm the implementation and effectiveness of the remedy.

8.6. COMMUNICATION OF RESULTS

On an annual basis, ~~an Auditor Letter of Compliance, prepared in accordance with the *FPKI Annual Review Requirements* document, on behalf of an Agency PMA shall be provided to the SSP.~~

~~On an annual basis, the SSP PMA shall~~CAs operating under this policy must submit an annual review package to the FPKIPA. This package ~~shall~~must be prepared by the ~~SSP~~CA's PMA, in accordance with the FPKI Annual Review Requirements document~~ and~~. The package must include an assertion that all PKI components have been audited ~~–~~including any components that may be separately managed and operated. The report ~~shall~~must identify the versions of this CP and the CPS used in the assessment. Additionally, where necessary, the results ~~shall~~must be communicated as set forth in Section 8.5 above.

Each agency must provide an Auditor Letter of Compliance for those PKI components that it operates to its issuing CA or directly to the FPKIPA.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

9.1.1. Certificate Issuance or Renewal Fees

~~No stipulation.~~

CAs operating under this policy must make this determination.

9.1.2. Certificate Access Fees

Section 2 of this policy requires that CA certificates be publicly available. CAs operating under this policy must not charge additional fees for access to this information.

9.1.3. Revocation or Status Information Access Fees

CAs operating under this policy must not charge additional fees for revoking certificates or access to CRLs and OCSP status information.

9.1.4. Fees for other Services

~~No stipulation.~~

CAs operating under this policy must make this determination.

9.1.5. Refund Policy

~~No stipulation.~~

CAs operating under this policy must make this determination.

9.2. Financial Responsibility

This CP contains no limits on the use of certificates issued by CAs under this policy. Rather, entities, acting as relying parties, ~~shall~~must determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.

9.2.1. Insurance Coverage

~~No stipulation.~~

CAs operating under this policy must make this determination.

9.2.2. Other Assets

~~No stipulation.~~

CAs operating under this policy must make this determination.

9.2.3. Insurance or Warranty Coverage for End-Entities

~~No stipulation.~~

CAs operating under this policy must make this determination.

9.3. Confidentiality of Business Information

CA information not requiring protection ~~shall~~must be made publicly available. Public access to organizational information ~~shall~~must be determined by the respective organization.

9.3.1. Scope of Confidential Information

~~No stipulation.~~

CAs operating under this policy must make this determination.

9.3.2. Information not within the Scope of Confidential Information

~~No stipulation.~~

CAs operating under this policy must make this determination.

9.3.3. Responsibility to Protect Confidential Information

~~No stipulation.~~

A CA must not disclose non-certificate information to any third party unless authorized by this policy, required by U.S. law, U.S. government rule or regulation, or order of a U.S. court of competent jurisdiction. The contents of the archives maintained by CAs operating under this policy must not be released except as required by this policy, required by U.S. law, U.S. government rule or regulation, or order of a U.S. court of competent jurisdiction.

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. Privacy Plan

~~The FPKIMA or Agency PMA shall conduct a Privacy Impact Assessment. If deemed necessary, the FPKIMA or Agency PMA shall have a Privacy Plan to protect personally identifying information (PII) from unauthorized disclosure. For the Common Policy Root CA, the FPKIPA shall approve the Privacy Plan. Privacy plans will be implemented~~CAs must conduct a Privacy Threshold Assessment, and implement and maintain any required Privacy Impact Assessments and Privacy Plans in accordance with the requirements of the Privacy Act of 1974, as amended.

9.4.2. Information Treated as Private

Federal entities acquiring services under this policy ~~shall~~must protect all Subscriber PII from unauthorized disclosure. Records of individual transactions may be released upon request of any Subscribers involved in the transaction or their legally recognized agents. The contents of the archives maintained by CAs operating under this policy ~~shall~~must not be released except as required by law.

Collection of PII ~~shall~~must be limited to the minimum necessary to validate the identity of the Subscriber. This may include attributes that correlate identity evidence to authoritative sources. The RA ~~shall~~must provide explicit notice to the Subscriber regarding the purpose for collecting and maintaining a record of the PII necessary for identity proofing and the consequences for not providing the information. PII collected for identity proofing purposes ~~shall~~must not be used for any other purpose.

9.4.3. Information not Deemed Private

Information included in certificates is not subject to protections outlined in Section 9.4.2~~. However, certificates that contain the FASC-N and/or UUID in the subject alternative name extension, such as PIV Authentication Certificates, shall not be distributed via public repositories (e.g., via LDAP or HTTP).~~, but may not be sold to a third party.

9.4.4. Responsibility to Protect Private Information

Sensitive information must be stored securely, and may be released only in accordance with other stipulations in Section 9.4.

All information collected as part of the identity proofing process ~~shall~~must be protected to ensure confidentiality and integrity. In the event ~~the Agency PMA~~an agency terminates PKI activities, it ~~shall~~must be responsible for disposing of or destroying sensitive information, including PII, in a secure manner, and maintaining its protection from unauthorized access until destruction.

9.4.5. Notice and Consent to Use Private Information

The FPKIMA or ~~Agency PMA~~an agency POC is not required to provide any notice or obtain the consent of the Subscriber or authorized agency personnel in order to release private information in accordance with other stipulations of Section 9.4.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

The FPKIMA or ~~Agency PMA shall~~an agency POC must not disclose private information to any third party unless authorized by this policy, required by law, government rule or regulation, or order of a court of competent jurisdiction. Any request for release of information ~~shall~~must be processed according to [41 CFR 105-60.605~~.~~].

9.4.7. Other Information Disclosure Circumstances

None.

9.5. INTELLECTUAL PROPERTY RIGHTS

~~The FPKIMA will~~CAs must not knowingly violate intellectual property rights held by others.

9.6. REPRESENTATIONS AND WARRANTIES

The obligations described below pertain to the FPKIMA and ~~Agency PMAs~~each issuing agency.

The FPKIPA ~~shall —~~must:

- Approve the CPS for each CA that issues certificates under this policy;
- Review periodic compliance audits to ensure that CAs are operating in compliance with their approved CPSs;
- Review ~~name space~~namespace control procedures to ensure that distinguished names are uniquely assigned for all certificates issued under this CP;
- Revise this CP to maintain the level of assurance and operational practicality;
- Publicly distribute this CP; and
- Coordinate modifications to this CP to ensure continued compliance by CAs operating under approved CPSs.

~~The Agency Policy Management Authorities shall —~~

Each issuing agency must:

- Review periodic compliance audits to ensure that RAs and other components operated by the agency are operating in compliance with their approved CPSs; and
- Review ~~name space~~namespace control procedures to ensure that distinguished names are uniquely assigned within their agency.

9.6.1. CA Representations and Warranties

CAs operating under this policy ~~shall~~must warrant that their procedures are implemented in accordance with this CP, and that any certificates issued that assert the policy OIDs identified in this CP were issued in accordance with the stipulations of this policy.

A CA that issues certificates that assert a policy defined in this document ~~shall~~must conform to the stipulations of this document, including~~—~~:

- Providing to the FPKIPA a CPS, as well as any subsequent changes, for conformance assessment.
- Maintaining its operations in conformance to the stipulations of the approved CPS.
- Ensuring that registration information is accepted only from approved RAs operating under an approved CPS.
- Including only valid and appropriate information in certificates, and maintaining evidence that due diligence was exercised in validating the information contained in the certificates.
- Revoking the certificates of Subscribers found to have acted in a manner counter to their obligations in accordance with Section 9.6.3.
- Operating or providing for the services of an on-line repository, and informing the repository service provider of their obligations if applicable.

9.6.2. RA Representations and Warranties

An RA that performs registration functions as described in this policy ~~shall~~must comply with the stipulations of this policy, and comply with a CPS approved by the FPKIPA for use with this policy. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities. An RA supporting this policy ~~shall~~must conform to the stipulations of this document, including~~—~~:

- Maintaining its operations in conformance to the stipulations of the approved CPS.
- Including only valid and appropriate information in certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate.
- Ensuring that obligations are imposed on Subscribers in accordance with Section 9.6.3, and that Subscribers are informed of the consequences of not complying with those obligations.

9.6.3. Subscriber Representations and Warranties

A Subscriber (or human sponsor for device certificates) ~~shall~~must be required to sign a document containing the requirements the Subscriber ~~shall~~must meet respecting protection of the private key and use of the certificate before being issued the certificate. Wherever possible, Subscriber documents must be digitally signed.

Subscribers ~~shall —~~must:

- Accurately represent themselves in all communications with the PKI authorities.
- Protect their private key(s) at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures.
- Promptly notify the appropriate CA upon suspicion of loss or compromise of their private key(s). Such notification ~~shall~~must be made directly or indirectly through mechanisms consistent with the CA’s CPS.
- Abide by all the terms, conditions, and restrictions levied on the use of their private key(s) and certificate(s).

If the human sponsor for a device is not physically located near the sponsored device, and/or does not have sufficient administrative privileges on the sponsored device to protect the device's private key and ensure that the device's certificate is only used for authorized purposes, the device sponsor may delegate these responsibilities to an authorized administrator for the device. ~~The delegation shall be documented and signed by both the device sponsor and the authorized administrator for the device. Delegation does not relieve the device sponsor of his or her accountability for these responsibilities.~~

9.6.4. Relying Parties Representations and Warranties

This CP does not specify the steps a relying party should take to determine whether to rely upon a certificate. The relying party decides, pursuant to its own policies, what steps to take.~~ The CA merely provides the tools (i.e., certificates and CRLs) needed to perform the trust path creation, validation, and CP mappings that the relying party may wish to employ in its determination.~~

9.6.5. Representations and Warranties of Other Participants

None.

9.7. Disclaimers of Warranties

CAs operating under this policy may not disclaim any responsibilities described in this CP.

9.8. Limitations of Liability

The U.S. Government ~~shall~~must not be liable to any party, except as determined pursuant to the [Federal Tort Claims Act (FTCA), 28 U.S.C. 2671-2680~~,~~], or as determined through a valid express written contract between the Government and another party.

9.9. Indemnities

No stipulation.

9.10. Term and Termination

9.10.1. Term

This CP becomes effective when approved by the FPKIPA. This CP has no specified term.

9.10.2. Termination

Termination of this CP is at the discretion of the FPKIPA.

9.10.3. Effect of Termination and Survival

The requirements of this CP remain in effect through the end of the archive period for the last certificate issued.

9.11. Individual Notices and Communications with Participants

The FPKIPA ~~shall~~must establish appropriate procedures for communications with CAs operating under this policy via contracts or memoranda of agreement as applicable.

For CAs operating under this policy, any planned changes to the infrastructure that ~~has~~have the potential to affect the FPKI operational environment ~~shall~~must be communicated to the FPKIPA at least two weeks prior to implementation~~, and~~. All new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the change must be provided to the FPKIPA within 24 hours following implementation.

For all other communications, no stipulation.

9.12. AMENDMENTS

9.12.1. Procedure for Amendment

The FPKIPA ~~shall~~must review this CP at least once every year. Corrections, updates, or changes to this CP ~~shall~~must be publicly available. Suggested changes to this CP ~~shall~~must be communicated to the contact in Section 1.5.2; such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

9.12.2. Notification Mechanism and Period

Proposed changes to this CP ~~shall~~must be distributed electronically to FPKIPA members and observers in accordance with the Charter and By-laws.

9.12.3. Circumstances under which OID must be Changed

OIDs will be changed if the FPKIPA determines that a change in the CP reduces the level of assurance provided.

9.13. DISPUTE RESOLUTION PROVISIONS

The FPKIPA ~~shall~~must facilitate the resolution between entities when conflicts arise as a result of the use of certificates issued under this policy. When the dispute is between federal agencies, and the FPKIPA is unable to facilitate resolution, dispute resolution may be escalated to ~~OMB or~~the White House Office of Management and Budget or to the U.S. Department of Justice, Office of Legal Counsel as necessary.

~~For CAs operating as Shared Service Providers, disputes as to operational or policy issues shall use the procedure set forth in the *Shared Service Provider Roadmap*.~~

9.14. GOVERNING LAW

The construction, validity, performance and effect of certificates issued under this CP for all purposes ~~shall~~must be governed by United States federal law (statute, case law, or regulation).

9.15. COMPLIANCE WITH APPLICABLE LAW

All CAs operating under this policy are required to comply with applicable law.

9.16. *Miscellaneous Provisions*

9.16.1. Entire Agreement

~~No stipulation.~~

CAs operating under this policy must make this determination.

9.16.2. Assignment

~~No stipulation.~~

CAs operating under this policy must make this determination.

9.16.3. Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP ~~shall~~must remain in effect until the CP is updated. The process for updating this CP is described in Section 9.12.

9.16.4. Enforcement (Attorneys' Fees and Waiver of Rights)

~~No stipulation.~~

CAs operating under this policy must make this determination.

9.16.5. Force Majeure

~~No stipulation.~~

CAs operating under this policy must make this determination.

9.17. *Other Provisions*

~~No stipulation.~~

~~10. Bibliography~~

~~The following documents were used in part to develop this CP:~~CAs operating under this policy must make this determination.

Appendix A: PIV and Common PIV Interoperable Comparison

Trust	Technical Requirements	PIV	PIV-I
~~ABADSG~~	~~Digital Signature Guidelines, 1996-08-01. http://itlaw.wikia.com/wiki/American_Bar_Association_(ABA)_Digital_Signature_Guidelines~~ Suitability Assurance: Favorably adjudicated National Agency Check with Inquiries (minimum) or other Tier 1 investigation	x	
~~APL~~	~~Approved Products List (APL) http://www.idmanagement.gov/approved-products-list-apl~~ PIV policy object identifier on PIV Authentication Certificates	x	
~~AUDIT~~	~~FPKI Annual Review Requirements~~ PIV-I equivalent policy object identifier on PIV-I Authentication Certificates		x
	PIV Content Signing object signing certificate	x	
	PIV-I Content Signing equivalent object signing certificate		x
~~CCP-PROF~~	~~X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program. http://www.idmanagement.gov/fpkipa/documents/CertCRLprofileForCP.pdf~~PIV Card Authentication Certificate	x	
~~CIMC~~	~~Certificate Issuing and Management Components Family of Protection Profiles, version 1.0, October 31, 2001. http://csrc.nist.gov/pki/documents/CIMC_PP_20011031.pdf~~		
~~E-Auth~~	~~E-Authentication Guidance for Federal Agencies, M-04-04, December 16, 2003. http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf~~PIV-I Card Authentication Certificate		x
~~FIPS 140-2~~	~~Security Requirements for Cryptographic Modules, FIPS 140-2, May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf~~Card must not be valid for more than 6 years and card expiration must not exceed the expiration date of object signing certificate	x	x

~~FIPS 186-4~~	~~Digital Signature Standard (DSS), FIPS 186-4, July 2013. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf~~		

~~FIPS 201-2~~**Credential Edg**	~~Personal Identity Verification (PIV) of Federal Employees and Contractors, FIPS 201-2, August 2013. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf~~Card stock certified by FIPS 201 Evaluation Program	x	x
~~FOIACT~~	~~5 U.S.C. 552, Freedom of Information Act. http://www4.law.cornell.edu/uscode/5/552.html~~Command edge and NIST SP 800-85 conformant	x	x
~~ISO9594-8~~	NIST SP 800-73 conformant data model and PIV Application Identifier (AID)~~ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.~~	x	x
	NIST SP 800-73 conformant to include GUID present in the CHUID	x	x
	RFC 4122 conformant UUID required in the GUID data element of the CHUID	x	x
	RFC 4122 conformant UUID present in the Authentication Certificates	x	x

Topography	FIPS 201 compliant topography	x	
	Minimally contains facial image, cardholder name, issuing organization, and expiration, but does not replicate FIPS 201 topography requirements		x
~~ITMRA~~**Card Management System**	~~40 U.S.C. 1452, Information Technology Management Reform Act of 1996. http://www4.law.cornell.edu/uscode/40/1452.html~~Card Management Master Key maintained in a FIPS 140-2 Level 2 Cryptographic Module and conforms to [NIST SP 800-78] requirements; activation of the Card Management Master Key requires commensurate authentication of Trusted Roles	x	x
~~NAG69C~~	~~Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.~~		

~~NSD42~~ ~~National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990.~~
~~http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt~~
~~(redacted version)~~

~~NS4005~~ ~~NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.~~

APPENDIX B: REFERENCES

ABADSG Digital Signature Guidelines, 1996-08-01. http://itlaw.wikia.com/wiki/American_Bar_Association_(ABA)_Digital_Signature_Guidelines

APL Approved Products List (APL) http://www.idmanagement.gov/approved-products-list-apl

AUDIT FPKI Annual Review Requirements https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-annual-review-requirements.pdf

CCP-PROF Common Policy X.509 Certificate and Certificate Revocation List (CRL) Profiles https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-x509-cert-profile-ssp.pdf

Executive Order 12968 Executive Order 12968 - Access to Classified Information https://www.govinfo.gov/content/pkg/FR-1995-08-07/pdf/95-19654.pdf

FIPS 140-2 Security Requirements for Cryptographic Modules, FIPS 140-2, May 25, 2001. https://csrc.nist.gov/publications/detail/fips/140/2/final

FIPS 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors, FIPS 201-2, August 2013. https://csrc.nist.gov/publications/detail/fips/201/2/final

ITMRA 40 U.S.C. 1452, Information Technology Management Reform Act of 1996. https://govinfo.library.unt.edu/npr/library/misc/itref.html

NS4009 NSTISSI 4009, National Information Systems Security Glossary, January 1999.

PACS *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems*, Version 2.~~2~~3, The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group, ~~July 30, 2004. http://www.idmanagement.gov/smartcard/information/TIG_SCEPACS_v2.2.pdf~~December 20, 2005. https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/TIG_SCEPACS_v2.3.pdf

PIV-I Issuers Personal Identity Verification Interoperability for Issuers

	https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/piv-i-for-issuers.pdf
PIV-I ~~Profiles~~Profile	X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards ~~https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-pivi-cert-profiles.pdf~~ https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-x509-cert-profiles-pivi.pdf
PKCS#1	Jakob Jonsson and Burt Kaliski, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, RFC 3447, February 2003. ~~http://www.ietf.org/rfc/rfc3447.txt~~http://www.ietf.org/rfc/rfc3447.txt
PKCS#12	PKCS #12~~ v1.0~~: Personal Information Exchange Syntax ~~June 24, 1999.~~ ~~ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf~~v1.1 July 2014. https://tools.ietf.org/html/rfc7292
RFC 2585	Internet X.509 Public Key Infrastructure: Operational Protocols: FTP and HTTP, Russel Housley and Paul Hoffman, May 1999. https://www.ietf.org/rfc/rfc2585.txt
RFC 3647	Certificate Policy and Certification Practices Framework, Chokhani and Ford, Sabett, Merrill, and Wu, November 2003. ~~http://www.ietf.org/rfc/rfc3647.txt~~http://www.ietf.org/rfc/rfc3647.txt
RFC 4122	A Universally Unique IDentifier (UUID) URN Namespace, Paul J. Leach, Michael Mealling, and Rich Salz, July 2005. ~~http://www.ietf.org/rfc/rfc4122.txt~~http://www.ietf.org/rfc/rfc4122.txt
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. ~~https://www.ietf.org/rfc/rfc5280.txt~~ https://www.ietf.org/rfc/rfc5280.txt
RFC 5322	Internet Message Format ~~http://www.ietf.org/rfc/rfc5322.txt~~ http://www.ietf.org/rfc/rfc5322.txt
RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. ~~https://tools.ietf.org/html/rfc6960~~ https://tools.ietf.org/html/rfc6960

RFC 8551
Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification, J. Schaad, B. Ramsdell, S. Turner, April 2019. https://tools.ietf.org/rfc/rfc8551.txt

SP 800-37
Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, NIST Special Publication 800-37, Revision ~~1, February 2010. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf~~2, December2018. https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

SP 800-56A
Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, NIST Special Publication 800-56A ~~http://csrc.nist.gov/publications/nistpubs/~~https://csrc.nist.gov/publications/detail/sp/800-56a/rev-3/final

SP 800-63-3
Digital Identity Guidelines ~~https://csrc.nist.gov/publications/detail/sp/800-63/3/final~~ https://csrc.nist.gov/publications/detail/sp/800-63/3/final

SP 800-~~73-3(1)~~76-2
~~Interfaces~~Biometric Specifications for Personal Identity Verification~~—Part 1: End-Point PIV Card Application Namespace, Data Model and Representation~~, NIST Special Publication 800-~~73-3, February 2010.~~76-2, July 2013. ~~http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART1_piv-card-applic-namespace-date-model-rep.pdf~~https://csrc.nist.gov/publications/detail/sp/800-76/2/final

SP 800-~~76~~78-4
~~Biometric Specifications~~Cryptographic Algorithms and Key Sizes for Personal Identity Verification, NIST Special Publication 800-~~76-2, July 2013.~~78-4, May 2015. ~~http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-76-2.pdf~~ https://csrc.nist.gov/publications/detail/sp/800-78/4/final

SP 800-79-2
Guidelines for the Accreditation of Personal Identity Verification Card Issuers, NIST Special Publication 800-79 ~~http://csrc.nist.gov/publications/nistpubs/~~ https://csrc.nist.gov/publications/detail/sp/800-79/2/final

SP 800-89
Recommendation for Obtaining Assurances for Digital Signature Applications, NIST Special Publication 800-89 ~~http://csrc.nist.gov/publications/nistpubs/~~https://csrc.nist.gov/publications/detail/sp/800-89/final

SP 800-157
Guidelines for Derived Personal Identity Verification (PIV) Credentials, NIST Special Publication 800-157. ~~http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf or~~

~~http://csrc.nist.gov/publications/drafts/800-157/sp800_157_draft.pdf~~
https://csrc.nist.gov/publications/detail/sp/800-157/final

X.509 ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

APPENDIX C: ACRONYMS AND ABBREVIATIONS

CA	Certification Authority
~~CAA~~	~~Certification Authority Authorization~~
~~C&A~~	~~Certification and Accreditation~~
CHUID	Card Holder Unique Identifier
~~COMSEC~~	~~Communications Security~~
~~CMS~~	~~Card Management System~~
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Objects Registry
DN	Distinguished Name
DPCI	Derived PIV Credential Issuer
ECDSA	Elliptic Curve Digital Signature Algorithm
EKU	Extended Key Usage
FPKIMA	Federal Public Key Infrastructure Management Authority
~~FIPS PUB~~	~~(US) Federal Information Processing Standards Publication~~
FPKI	Federal Public Key Infrastructure
~~FPKIA~~	~~Federal PKI Architecture~~
FPKIPA	Federal PKI Policy Authority
FQDN	Fully Qualified Domain Name
HTTP	Hypertext Transfer Protocol
~~IEC~~	~~International Electrotechnical Commission~~
IETF	Internet Engineering Task Force

IP	Internet Protocol
KRP	Key Recovery Policy
KRPS	Key Recovery Practice Statement
LDAP	Lightweight Directory Access Protocol
ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
~~ITU~~	~~International Telecommunications Union~~
~~ITU-T~~	~~International Telecommunications Union – Telecommunications Sector~~
NARA	U.S. National Archives and Records Administration
NIST	National Institute of Standards and Technology
NSA	National Security Agency
~~NSTISSI~~	~~National Security Telecommunications and Information Systems Security Instruction~~
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PCI	PIV Card Issuer
PII	Personal Identifying Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification Interoperable
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PSS	Probabilistic Signature Scheme
RA	Registration Authority
RDN	Relative Distinguished Name

RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
RSASSA	RSA Signature Scheme with Appendix
SHA	Secure Hash Algorithm
S/MIME	Secure/Multipurpose Internet Mail Extensions
SP	Special Publication
~~SSL~~	~~Secure Sockets Layer~~
SSP-REP	Shared Service Provider Repository Service Requirements
~~TSA~~TLS	~~Time Stamp Authority~~Transport Layer Security
~~UPS~~	~~Uninterrupted Power Supply~~
URL	Uniform Resource Locator
U.S.C.	United States Code
UUID	Universal Unique Identifier
VM	Virtual Machine
VME	Virtual Machine Environment
WWW	World Wide Web

Appendix D: Glossary

Access — Ability to make use of any information system (IS) resource. [NS4009]

Access Control — Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]

Accreditation — Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]

Activation Data — Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).

Applicant

The Subscriber is sometimes also called an "Applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]

Archive

Long-term, physically separate storage.

~~Attribute Authority~~

~~An entity, recognized by the FPKIPA or comparable body as having the authority to verify the association of attributes to an identity.~~

Audit

Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]

Audit Data

Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]

Authenticate

To confirm the identity of an entity when that identity is presented.

Authentication

Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]

Backup

Copy of files and programs made to facilitate recovery if necessary. [NS4009]

Binding

Process of associating two related elements of information. [NS4009]

Biometric

A physical or behavioral characteristic of a human being.

Certificate

A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]. As used in this CP, the term “certificate” refers to X.509 certificates that expressly reference the OID of this CP in the certificatePolicies extension.

Certification Authority (CA)

An authority trusted by one or more users to issue and manage X.509 public key certificates and CRLs.

CA Facility

The collection of equipment, personnel, procedures and structures that are used by a certification authority to perform certificate issuance and revocation.

Certification Authority Software

Key management and cryptographic software used to manage certificates issued to Subscribers.

Certificate Policy (CP)

A certificate policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A certificate policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

Certification Practice Statement (CPS)

A statement of the practices that a CA employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).

Certificate-Related Information

Information, such as a Subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.

Certificate Revocation List (CRL)

A list maintained by a certification authority of the certificates that it has issued that are revoked prior to their stated expiration date.

Certificate Status Server (CSS)

A trusted entity that provides on-line verification to a relying party of a subject certificate's revocation status~~, and may also provide additional attribute information for the subject certificate.~~.

Client (application)

A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server.

~~Common Criteria~~

~~A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.~~

Compromise

Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]

Computer Security Objects Registry (CSOR)

Computer Security Objects Registry operated by the National Institute of Standards and Technology.

Confidentiality

Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]

Cross-Certificate

A certificate used to establish a trust relationship between two certification authorities.

Cryptographic Module

The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS 140~~-2~~]

Data Integrity

Assurance that the data are unchanged from creation to reception.

Device

A non-person entity, i.e., a piece of hardware or a software application

Digital Signature

The result of a transformation of a message by means of a cryptographic system using keys such that a relying party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.

~~Dual Use Certificate~~

~~A certificate that is intended for use with both digital signature and data encryption services.~~

Encryption Certificate

A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.

~~End Entity Certificate~~

~~A certificate in which the subject is not a CA.~~

FPKI Management Authority (FPKIMA)

The Federal Public Key Infrastructure Management Authority is the organization responsible for operating the Federal Common Policy ~~Root~~ Certification Authority.

Federal Public Key Infrastructure Policy Authority (FPKIPA)

The FPKIPA is a Federal Government body responsible for setting, implementing, and administering policy decisions regarding the Federal PKI Architecture.

Firewall

Gateway that limits access between networks in accordance with local security policy. [NS4009]

~~High Assurance Guard (HAG)~~

~~An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.~~

Hypervisor

Computer software, firmware or hardware that creates and runs virtual machines. ~~A hypervisor uses native execution~~A hypervisor uses native execution to share and manage hardware, allowing for multiple environments which are isolated from one another, yet exist on the same physical machine. Also known as an isolation kernel or virtual machine monitor.

Information Systems Security Officer (ISSO)

Person responsible to the Designated Approving Authority for ensuring the security of an information system throughout its life-cycle, from design through disposal. [NS4009]

~~Inside Threat~~

~~An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.~~

Integrity

Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.

Intellectual Property

Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.

Intermediate CA

A CA that is subordinate to another CA, and has a CA subordinate to itself.

Key Escrow

A deposit of the private key of a Subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the Subscriber, the terms of which require one or more agents to hold the Subscriber's private key for the benefit of the Subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]

Key Exchange

The process of exchanging public keys in order to establish secure communications.

Key Generation Material

Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.

Key Pair

Two mathematically related keys having the properties that (1) one (public) key can be used to encrypt a message that can only be decrypted using the other (private) key, and (2) even knowing the public key, it is computationally infeasible to discover the private key.

Key Recovery Policy (KRP)

A key recovery policy is a specialized form of administrative policy tuned to the protection and recovery of key management private keys (i.e. decryption keys) held in escrow. A key recovery policy addresses all aspects associated with the storage and recovery of key management certificates.

Key Recovery Practices Statement (KRPS)

A statement of the practices that a Key Recovery System employs in protecting and recovering key management private keys, in accordance with specific requirements (i.e., requirements specified in the KRP).

~~Legacy Federal PKI~~

~~A PKI Implementation owned and managed by a Federal Agency and cross-certified with the Federal Bridge prior to 12/31/2005.~~

Modification (of a certificate)

The act or process by which data items bound in an existing public key certificate~~, especially authorizations granted to the subject,~~ are changed by issuing a new certificate.

Mutual Authentication

Occurs when parties at both ends of a communication activity authenticate each other (see authentication).

~~Naming Authority~~

~~An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.~~

National Security System

Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]

Network Guard

An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.

Non-Repudiation

Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a relying party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key.

Object Identifier (OID)

A specialized formatted number that is registered with an internationally recognized standards organization, the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the Federal PKI, OIDS are used to uniquely identify certificate policies and cryptographic algorithms.

Offline CA

An offline certification authority is a certification authority isolated from network access, and is often kept in a powered-down state.

Out-of-Band

Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring on-line).

~~Outside Threat~~

~~An unauthorized entity from outside the domain perimeter that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.~~

Physically Isolated Network

A network that is not connected to entities or systems outside a physically controlled space.

PKI Sponsor

Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.

Policy Management Authority (PMA)

The individual or group that is responsible for the creation and maintenance of Certificate Policies and Certification Practice Statements, and for ensuring that all Entity PKI components (e.g., CAs, CSSs, ~~CMSs~~Card Management Systems, RAs) are audited and operated in compliance with the entity PKI CP. The PMA evaluates non-domain policies for acceptance within the domain, and generally oversees and manages the PKI certificate policies. For the Common Policy, the PMA is the FPKIPA.

Privacy

Restricting access to Subscriber or relying party information in accordance with federal law.

Private Key

(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.

Public Key

(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to

encrypt confidential information. In both cases, this key is normally made publicly available in the form of a digital certificate.

Public Key Infrastructure (PKI)

A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public/private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Registration Authority (RA)

An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).

Re-key (a certificate)

To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate that contains the new public key.

Relying Party

A person or entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.

Renew (a certificate)

The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.

Repository

A ~~database~~system containing ~~information and~~ data relating to certificates or revocation data as specified in this CP~~; may also be referred~~. May refer to ~~as~~ a directory, web server, or server which only hosts pre-generated OCSP responses.

Revoke a Certificate

To prematurely end the operational period of a certificate effective at a specific date and time.

Risk

An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Risk Tolerance

The level of risk an entity is willing to assume in order to achieve a potential desired result.

Root CA

In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.

Server

A system entity that provides a service in response to requests from clients.

Signature Certificate

A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

Structural Container

An organizational unit attribute included in a distinguished name solely to support local directory requirements, such as differentiation between Human Subscribers and devices.

Subordinate CA

In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).

Subscriber

A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual, an application or network device.

Superior CA

In a hierarchical PKI, a CA that has certified the certificate signature key of another CA, and that constrains the activities of that CA. (See subordinate CA).

Supervised Remote Identity Proofing

A real-time identity proofing event where the RA/Trusted Agent is not in the same physical location as the Applicant/Subscriber. The RA/Trusted Agent controls a device which is utilized by the Applicant/Subscriber in order to ensure the remote identity proofing process employs physical, technical and procedural measures to provide sufficient confidence that the remote session can be considered equivalent to a physical, in-person identity proofing process. Supervised Remote Identity Proofing must meet the criteria specified in NIST SP 800-63A Section 5.3.3; and must have the capacity to capture an approved biometric.

~~System Equipment Configuration~~

~~A comprehensive accounting of all system hardware and software types and settings.~~

~~System High~~

~~The highest security level supported by an information system. [NS4009]~~

Threat

Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]

~~Time Stamp Authority~~

~~An independent, reliable service that issues and verifies electronic time stamps.~~

Trust List

Collection of Trusted Certificates used by relying parties to authenticate other certificates.

Trusted Agent

Entity authorized to act as a representative of a CA in confirming Subscriber identification during the registration process. Trusted agents do not have automated interfaces with certification authorities.

Trusted Certificate

A certificate that is trusted by the relying party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".

~~Trusted Timestamp~~

~~A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.~~

Trustworthy System

Computer hardware, software, and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.

Two-Person Control

Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements. [NS4009]

Virtual Machine Environment

An emulation of a computer system (in this case, a CA) that provides the functionality of a physical machine in a platform-independent environment. They provide functionality needed to execute entire operating systems. At this time, allowed VMEs are limited to Hypervisor type virtual environments. Other technology, such as Docker Containers, is not permitted.

Zeroize

A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS 140~~-2~~]

~~11. Acknowledgments~~

~~The Certificate Policy Working Group developed this CP based on RFC 3647 and the original U.S. Federal PKI Common Policy Framework Certificate Policy.~~

~~Appendix A – PIV and Common PIV Interoperable (Common PIV-I) Comparison~~

[illegible]	~~Technical Requirements~~	~~PIV~~	~~PIV-I~~
	~~Suitability Assurance:~~ ~~Favorably adjudicated National Agency Check with Inquiries (minimum) or other Tier 1 investigation~~	~~x~~	
	~~PIV policy object identifier on PIV Authentication Certificates~~	~~x~~	
	~~PIV-I equivalent policy object identifier on PIV-I Authentication Certificates~~		~~x~~
	~~PIV Content Signing object signing certificate~~	~~x~~	
	~~PIV-I Content Signing equivalent object signing certificate~~		~~x~~
	~~PIV Card Authentication Certificate~~	~~x~~	
	~~PIV-I Card Authentication Certificate~~		~~x~~
	~~Card shall not be valid for more than 6 years and card expiration shall not exceed the expiration date of object signing certificate~~	~~x~~	~~x~~
~~Credential Edge~~	~~Card stock certified by FIPS 201 Evaluation Program~~	~~x~~	~~x~~
	~~Command edge and NIST SP 800-85 conformant~~	~~x~~	~~x~~
	~~NIST SP 800-73 conformant data model and PIV Application Identifier (AID)~~	~~x~~	~~x~~
	~~NIST SP 800-73 conformant to include GUID present in the CHUID~~	~~x~~	~~x~~
	~~RFC 4122 conformant UUID required in the GUID data element of the CHUID~~	~~x~~	~~x~~
	~~RFC 4122 conformant UUID present in the Authentication Certificates~~	~~x~~	~~x~~

~~Topography~~	~~FIPS 201 compliant topography~~	~~x~~	
	~~Minimally contains facial image, cardholder name, issuing organization, and expiration, but does not replicate FIPS 201 topography requirements~~		~~x~~
~~Card Management System~~	~~Card Management Master Key maintained in a FIPS 140-2 Level 2 Cryptographic Module and conforms to [NIST SP 800-78] requirements; activation of the Card Management Master Key requires commensurate authentication of Trusted Roles~~	~~x~~	~~x~~